POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Un cadre de gouvernance pour la gestion intégrée des risques chez les organisations de grande ampleur

MORABITO LUCIANO

Département de mathématiques et de génie industriel

Thèse présentée en vue de l'obtention du diplôme de *Philosophiæ Doctor*

Génie industriel

Août 2025

© Luciano Morabito, 2025.

POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Cette thèse intitulée :

Un cadre de gouvernance pour la gestion intégrée des risques chez les organisations de grande ampleur

présentée par **Luciano MORABITO**

en vue de l'obtention du diplôme de *Philosophiæ Doctor*

a été dûment acceptée par le jury d'examen constitué de :

Mario BOURGAULT, président

Benoît ROBERT, membre et directeur de recherche

Dragan KOMLJENOVIC, membre externe

Frédéric PETIT, membre externe

DÉDICACE

Plus qu'une destination, le doctorat est une aventure. Un parcours sinueux jonché de plusieurs épreuves qui demande un investissement considérable. C'est un investissement certes financier, mais c'est surtout un investissement en temps. Que ce soit le temps investi dans la recherche ou dans la rédaction, le temps investi avec (et par) les personnes avec lesquelles nous avons l'opportunité de travailler, mais surtout, le temps investi dans les réflexions plus profondes quant à l'orientation à donner aux travaux. Réflexions qui parfois aboutissent rapidement, mais qui, le plus souvent du temps, nous conduisent vers des moments de remise en question profonde quant aux avenues possibles qui permettront de trouver une solution originale à la problématique identifiée et qui, au bout du compte, permettront de donner un sens à ce que l'on fait, donc, à cet investissement.

Ce temps si précieux investi dans le doctorat est évidemment du temps que nous ne pouvons dédier ailleurs, et principalement aux personnes qui nous sont les plus chères et que nous aimons plus que tout au monde. Ainsi, je dédie cette thèse à ma famille. À mes parents, pour m'avoir toujours encouragé à donner le meilleur de moi-même malgré les obstacles ; à ma conjointe, pour m'avoir constamment soutenu tout au long de cette aventure ; finalement, à mes enfants, pour leur patience, eux qui n'ont probablement pas pu profiter des dernières années autant qu'ils l'auraient souhaité. J'espère, que par cette aventure, j'aurai pu les inspirer à poursuivre leurs objectifs jusqu'au bout et à ne jamais abandonner.

REMERCIEMENTS

S'il y a un terme qui selon moi explique le mieux ce qu'est un doctorat, c'est l'humilité. Avoir l'humilité de reconnaître que ce que ce nous avons fait, nous ne l'avons pas fait seul ; que certaines idées viennent de nous, mais que plusieurs viennent des autres. Oui, nous avons été capables d'identifier une problématique et d'y proposer une solution originale, mais cette solution que nous avons pu porter en avant vient des nombreuses réflexions que nous avons pu avoir parce qu'elles ont été alimentées par les discussions que nous avons eues avec nos collègues, nos amis, les membres de notre famille, mais surtout, par les réflexions faites par une communauté de chercheurs engagés qui ont partagé leurs idées, leurs succès, voire même, dans certains cas, leurs échecs, avec un objectif noble et altruiste de faire évoluer la connaissance pour le bien-être collectif des générations actuelles et futures. Les résultats d'un doctorat ne sont donc pas attribuables uniquement au travail de leur auteur. Ils sont le fruit d'une réflexion collective à laquelle nous nous sommes joints afin d'y apporter une contribution supplémentaire.

Ainsi, mes remerciements vont à toutes les personnes qui ont pu alimenter mes réflexions au cours des dernières années. Principalement, je remercie mon directeur de recherche, Pr Benoît Robert pour avoir supervisé mes travaux de doctorat. C'est avec Benoît que j'ai commencé ma carrière professionnelle dans le domaine des risques il y a plus de 20 ans, au *Centre Risque & Performance*, et n'eût été de lui, je n'aurais possiblement jamais découvert cet univers si passionnant.

Je remercie également Cathy G., directrice de la direction « Sûreté et résilience de l'entreprise » au sein de l'organisation partenaire pour avoir cru en cette initiative et pour m'avoir accordé sa confiance. Je remercie aussi les gestionnaires des unités fonctionnelles qui ont participé à ce projet (Josée C., Dave C., Timothy F., Michael F., Rubina K., François M., et Patrick T.) et les experts qui ont fait partie, à un moment ou à un autre, de l'équipe de projet (Joanne A., Frédéric G.-P., Geneviève L., Jennifer L., Rachel L., Carol M., Phillip P., Étienne R. et Michael S.). L'approche présentée dans cette thèse est le fruit d'un travail hautement collaboratif qui n'aurait pu avoir lieu sans la participation de toutes ces personnes.

Finalement, je remercie Zofia L. pour la traduction des articles présentés dans cette thèse, et bien évidemment, les membres du jury, Pr Mario Bourgault, Dr Dragan Komljenovic et Dr Frédéric Petit pour avoir accepté d'évaluer cette thèse et pour le temps qu'ils y ont consacré.

PRÉAMBULE

J'ai commencé ma carrière professionnelle dans le domaine des risques au *Centre risque & performance* (CRP) de Polytechnique Montréal, en 2004. Créé et dirigé par le professeur Benoît Robert, le CRP a été mis sur pied après la Crise du verglas qui a frappé le Québec en janvier 1998. Son principal sujet de recherche : les interdépendances entre les Infrastructures Critiques (IC)[1].

Le CRP a été un précurseur de l'étude des interdépendances entre les IC puisque ce n'est qu'en 2001 que ce sujet a réellement pris une envergure internationale. Ce sont en fait les attentats terroristes du 11 septembre 2001 sur le World Trade Center de New York qui ont mis en lumière cette grande vulnérabilité de nos sociétés modernes et qui lui ont donné une perspective mondiale. Ce sujet complexe, en pleine émergence, devenait alors une priorité pour de nombreux pays, dont le Canada.

Alors que la problématique des interdépendances entre les IC était principalement abordée sous l'angle du développement d'outils informatiques, le CRP s'est particulièrement distingué dans ses travaux en misant sur la coopération multiorganisationnelle. Parce que les interdépendances étaient un sujet encore peu connu, le CRP faisait le pari qu'en combinant l'expertise et les connaissances de l'équipe de recherche et des acteurs du terrain, et en intégrant les contraintes des organisations liées à la confidentialité des informations, il allait parvenir à développer un modèle d'analyse des interdépendances entre les IC qui serait valide autant en théorie, qu'en pratique.

Ce pari porta ses fruits. Si bien qu'après trois années de travaux, le CRP développait une méthodologie d'identification et de caractérisation des interdépendances entre les IC bien structurée et basée sur une approche tous risques novatrice : l'approche par conséquences ; après six années, le CRP développait DOMINO : un outil capable de modéliser les interdépendances entre les IC et de simuler les effets domino engendrés par leur défaillance en y intégrant un paramètre pratiquement jamais utilisé dans le concept de risque : le temps.

---

[1] L'étude des interdépendances entre les IC consiste à analyser et comprendre la dynamique des relations de dépendances qui lient ces infrastructures entre elles. Ces interdépendances sont dues aux échanges de ressources entre ces infrastructures et sont à la base de phénomènes d'effets domino difficilement prévisibles pouvant se produire à la suite de la défaillance d'une infrastructure ou d'un équipement d'une IC. Profitant des vulnérabilités des systèmes, cette défaillance peut alors se propager dans le temps et dans l'espace et affecter l'ensemble des infrastructures et des activités socio-économiques d'une région ou d'un pays, voire plusieurs.

Pourquoi cette longue introduction sur DOMINO ? Si DOMINO a été un succès sur le plan de la recherche et du développement, avec une reconnaissance à l'échelle internationale, le transfert au milieu preneur n'a pas eu autant de succès et la coopération entre les IC du Québec, formée et entretenue par le CRP pendant près de 20 ans, n'a pas survécu. La question de savoir pourquoi DOMINO n'a pu aller plus loin a continué à alimenter mes réflexions alors que je poursuivais ma carrière dans le secteur privé. Comment, après avoir mis sur pied une initiative aussi ambitieuse et après y avoir consacré autant de temps et d'énergie, celle-ci pouvait-elle se terminer ainsi ?

Avec le recul que m'ont permis ces dernières années en travaillant en dehors d'un contexte de recherche, j'ai réalisé que la démarche que le CRP avait développée était en quelque sorte en avance sur son temps. Même si le CRP avait travaillé directement avec le milieu preneur, l'approche développée demande une certaine adaptation, voire un changement de culture, quant à la manière dont les organisations gèrent les risques. Lorsque je me suis joins à l'équipe de gestion des risques de l'organisation pour laquelle je travaille, j'ai été confronté à la réalité : DOMINO ne pouvait pas aller plus loin parce que les organisations n'en sont pas encore rendues là dans leur cheminement relatif à la gestion des risques. Comme celles-ci n'ont pas l'habitude de gérer leurs risques de manière réellement intégrée, leur demander de gérer leurs risques de manière intégrée et multiorganisationnelle ne pouvait pas fonctionner, surtout sans qu'une entité compétente n'ait le mandat d'animer cette coopération sur le long terme. Pourtant, les défis liés aux nouveaux risques auxquels sont confrontées les organisations, et plus généralement la société, et qui sont qualifiés d' « émergents », demandent ce genre d'approche.

Ainsi, le passage du milieu de la recherche à un milieu plus « opérationnel » m'a permis de constater que le défi lié à la gestion intégrée des risques n'est pas technique ou technologique, il est plutôt organisationnel et humain. Il en est un de gouvernance relatif à la manière dont les organisations gèrent les risques. Or, cette manière dont les organisations gèrent les risques représente elle-même un risque encore plus grand que les risques qu'elles tentent de gérer. Ainsi, avec les connaissances et l'expérience acquises sur plus de 20 ans, autant dans un contexte de recherche que dans un contexte plus opérationnel, j'ai décidé de réaliser des études doctorales dont le résultat est cette thèse qui propose un cadre de gouvernance pour la gestion intégrée des risques chez les organisations de grande ampleur. Ce cadre s'inspire du même principe fondamental sur lequel reposait DOMINO, c'est-à-dire la coopération, mais il a été adapté afin de pouvoir être appliqué à l'interne des grandes organisations.

RÉSUMÉ

Les organisations font face à des changements importants de leur environnement qui font apparaître de nouveaux risques. Qualifiés d' « émergents », ces risques sont caractérisés par un plus haut niveau d'incertitude, d'ambiguïté et de complexité qui fait en sorte qu'ils peuvent difficilement être adressés via les processus usuels de gestion des risques. Pour faire face à ces nouveaux risques, des approches plus multidisciplinaires et transversales de gestion des risques, dites « intégrées », sont nécessaires.

La Gestion Intégrée des Risques (GIR) est une problématique qui concerne davantage les grandes organisations. En effet, ce défi ne se pose pas particulièrement dans le contexte des petites organisations. Dans ces cas, la gestion des risques est souvent sous la responsabilité de quelques acteurs (voire, une seule équipe) et elle s'en retrouve donc, de soi, intégrée. En revanche, chez les grandes organisations, la gestion des risques est généralement scindée et répartie entre plusieurs Unités Fonctionnelles (UF) relativement indépendantes, chacune responsable de gérer une Activité liée à la Gestion des Risques (AGR), comme la continuité des affaires, les mesures d'urgence, la sécurité physique, la sécurité de l'information ou la santé et la sécurité au travail, par exemple. Or, lorsque plusieurs parties prenantes sont impliquées dans la même entreprise, une solide gouvernance doit être établie afin de s'assurer que chacune d'elles comprenne bien ses rôles et ses responsabilités (et celles des autres) dans l'entreprise commune et, surtout, afin de s'assurer de la coordination, la complémentarité et la cohérence des décisions qu'elles prennent et des actions qu'elles posent.

Ce projet de recherche doctorale explore cette problématique de la GIR chez les grandes organisations. Plus spécifiquement, il propose un cadre de gouvernance pour la GIR chez les organisations de grande ampleur. Ce cadre de gouvernance est basé sur le concept d'Espace de Coopération (EC) développé par le CRP dans le cadre du projet DOMINO et repose sur trois grands piliers : un référentiel commun, une structure de coopération et un modèle d'agrégation des Informations et des Connaissances, mais aussi des Incertitudes et des Inconnus (ICII) sur les risques.

Concernant le référentiel commun, le cadre propose aux grandes organisations d'adopter un concept de risque transversal qui permettra aux UF responsables des AGR d'établir une

Représentation Mentale Commune (RMC) (donc, une vision et une compréhension communes) de ce qu'est le risque et de visualiser à quels niveaux se situent leurs rôles et leurs responsabilités en lien avec la GIR, et plus spécifiquement, en lien avec les Mesures de Mitigation et Contrôles (MMC) qui sont déployées pour réduire les risques. Il propose également la mise en place d'un Cadre de Référence Commun (CRC) à l'ensemble des acteurs au sein de ces UF qui vise à s'assurer que toutes les décisions et les actions qui sont prises par ces acteurs sont clairement balisées et s'inscrivent dans une logique autant fonctionnelle qu'organisationnelle. Concernant la structure de coopération, le cadre recommande que la GIR soit sous la responsabilité d'une équipe multidisciplinaire compétente et entièrement dédiée. Cette équipe a pour mission d'assurer le lien et la coordination entre toutes les UF responsables des AGR, mais aussi entre les niveaux opérationnel, tactique et stratégique de l'organisation. Finalement, en ce qui concerne le modèle d'agrégation des ICII sur les risques, comme son nom l'indique, celui-ci a pour objectif d'agréger l'ensemble des ICII sur les risques qui sont réparties dans l'organisation afin d'en tirer une connaissance collective à plus forte valeur ajoutée capable de mieux supporter les processus de prise de décisions plus tactiques et stratégiques relatifs à la gestion des risques.

L'originalité du cadre de gouvernance proposé dans cette thèse naît en partie du concept de risque sur lequel il est basé. En effet, plutôt que d'utiliser le concept de risque issu des sciences exactes (et reposant sur la probabilité d'occurrence d'un aléa), celui-ci repose sur le concept de risque basé sur l'incertitude. Dans cette optique, où le risque est associé à une incertitude, réduire le risque ne revient plus à réduire la probabilité d'occurrence d'un aléa (paramètre sur lequel l'organisation a bien souvent peu de contrôle), mais plutôt à accroître la connaissance collective transversale (transdisciplinaire) des risques auxquels l'organisation est confrontée. Cette connaissance collective permet alors aux acteurs responsables de la GIR d'obtenir une compréhension commune plus large sur les risques qui contribue à une prise en charge cohérente et concertée de ces risques, mettant de l'avant les deux concepts qui sont au coeur de ce cadre de gouvernance, à savoir, le socioconstructivisme et l'intelligence situationnelle partagée.

Ce projet de recherche a été conduit en deux volets menés en parallèle : un volet théorique, visant à poser les concepts sous-tendant le cadre de gouvernance, et un volet pratique, visant à traduire ces concepts en outils concrets applicables dans les grandes organisations. Pour cela, les travaux ont été conduits en partenariat avec une grande organisation canadienne. Mettant de l'avant une méthodologie de recherche de type recherche-intervention, les travaux réalisés au sein de cette

organisation ont permis de développer un cadre de gouvernance qui est non seulement valide en théorie, mais qui est également opérationnel, c'est-à-dire qui est aussi valide en pratique.

Malgré certaines limitations, ce projet de recherche démontre la valeur ajoutée que la mise en place d'un cadre de gouvernance pour la GIR peut apporter aux grandes organisations. Il ouvre aussi la voie vers des manières plus efficaces et proactives, possiblement basées sur l'utilisation d'algorithmes informatiques ou l'intelligence artificielle, de gérer les risques, dont les risques émergents. Plus généralement, ce projet de recherche pourrait permettre à des initiatives de GIR multiorganisationnelles comme DOMINO de renaître.

Mots clés : cadre de gouvernance, cadre opérationnel commun, gestion intégrée des risques, incertitude, intelligence situationnelle partagée, organisation de grande ampleur, représentation mentale commune, risque émergent, socioconstructivisme.

ABSTRACT

Organizations are facing significant changes in their environment that are giving rise to new risks. Described as “emerging,” these risks are characterized by a higher level of uncertainty, ambiguity and complexity that makes them difficult to address through standard risk management processes. To address these new risks, more multidisciplinary and cross-functional risk management approaches, known as “integrated,” must be implemented by organizations.

Integrated risk management (IRM) is an issue that is more relevant to large organizations. Indeed, this challenge does not particularly arise in the context of small organizations. In these cases, risk management is often the responsibility of a few actors (even a single team) and is therefore inherently integrated. On the other hand, in large organizations, risk management is generally distributed among several functional units, each responsible for managing an operational activity related to risks, such as business continuity, emergency measures, physical security, information security or occupational health and safety, for example. However, when several stakeholders are involved in the same undertaking, a solid governance must be established to ensure that each of them understands their roles and responsibilities (and those of the others) and, above all, to ensure the coordination and coherence of the decisions they make and the actions they take.

This doctoral research project explores this issue of IRM in large organizations. More specifically, it proposes a governance framework for IRM in large organizations. This governance framework is based on the concept of Cooperative Space (CS) developed by the CRP as part of the DOMINO project and is based on three pillars: a common repository, a cooperative structure and an aggregation model for information and knowledge, but also uncertainties and unknowns on risks.

Regarding the common repository, the framework proposes that large organizations adopt a transversal risk concept that will allow the Organizational Units (OUs) responsible for managing an Activity related to Risk Management (ARM) to visualize at what level their roles and responsibilities are in relation to risk management, and more specifically, in relation to the Mitigation and Control Measures (MCMs) that are deployed to reduce risks. It also proposes the establishment of a Common Frame of Reference (CFR) for all stakeholders within these OUs, which aims to ensure that all decisions and actions taken by these stakeholders are clearly marked out and are consistent both at the organizational and functional levels. Regarding the cooperative

structure, the framework recommends that IRM be under the responsibility of a fully dedicated multidisciplinary team. This team's mission is to ensure the linkage between all OUs responsible for ARM, but also between the operational, tactical and strategic levels of the organization. Finally, regarding the aggregation model, as its name suggests, its objective is to allow information and knowledge, but also uncertainties and unknowns on risks that are distributed throughout the organization to be aggregated to derive collective knowledge with higher added value capable of better supporting decision-making processes relating to risk management.

The originality of this governance framework arises from the concept of risk on which it is based. Indeed, rather than using the concept of risk arising from the exact sciences (and based on the probability of occurrence of a hazard), it is based on the concept of risks based on uncertainty. From this perspective, reducing risk no longer means reducing the probability of occurrence of a hazard (a parameter over which organizations often have very little control), but rather increasing the collective cross-functional knowledge and understanding of the organization regarding the risks it faces, highlighting the two concepts at the heart of this governance framework, namely, social constructivism and shared situational awareness.

This research project was conducted in two parallel parts: a theoretical part, aimed at establishing the concepts underlying the governance framework, and a practical part aimed at translating these concepts into concrete tools applicable in large organizations. To this end, the work was conducted in partnership with a large Canadian organization. Putting forward an intervention research methodology, the work carried out within this organization has made it possible to develop a governance framework that is not only theoretically valid but is also operational (meaning that it is also valid in practice).

Despite some limitations, this research project demonstrates the added value that implementing a governance framework for IRM can bring to large organizations. It also paves the way for more efficient and proactive ways, possibly based on the use of computer algorithms or artificial intelligence, to manage their risks, including emerging risks. More generally, this could allow multi-organizational IRM initiatives like DOMINO to be revived.

Keywords: common operational framework, emerging risk, integrated risk management, governance framework, large organization, shared mental model, shared situational awareness, social constructivism, uncertainty.

TABLE DES MATIÈRES

DÉDICACE III

REMERCIEMENTS IV

PRÉAMBULE V

RÉSUMÉ VII

ABSTRACT X

TABLE DES MATIÈRES XII

LISTE DES TABLEAUX XVII

LISTE DES FIGURES XX

LISTE DES SIGLES ET ABRÉVIATIONS XXIII

CHAPITRE 1 INTRODUCTION 1

CHAPITRE 2 ARTICLE 1 : SUCCESS FACTORS AND LESSONS LEARNED DURING THE IMPLEMENTATION OF A COOPERATIVE SPACE FOR CRITICAL INFRASTRUCTURES 7

2.1 Mise en contexte et présentation de l'article 7

2.2 Abstract 8

2.3 Introduction 9

2.3.1 Interdependencies among CIs: a source of unpredictable DEs 9

2.3.2 Information sharing: a real challenge for collaborative approaches 10

2.4 Cooperative space: a model of collaboration dedicated to exchanges of information among multiple organisations 11

2.4.1 The cooperative space: an environment that fosters information exchange among Cis 11

2.4.2 DOMINO: A Des simulation tool resulting from the works of the Québec CS 13

2.5 Success factors associated with the implementation of a CS 17

2.5.1 A clear mandate resulting from a real problem 17

2.5.2 A competent moderator with demonstrated leadership skills 18

2.5.3 An approach that respects organisations' confidentiality constraints 19

2.6 Lessons learned from the DOMINO initiative: the difficulty of maintaining a CS over the long-term 20

2.6.1 A sustainable governance structure 20

2.6.2 Ongoing results to keep participants interested 21

2.6.3 Trust based on the creation of a win-win context 22

2.6.4 Measurable gains for the collaborating organisations 23

2.7 Discussion and conclusion 25

CHAPITRE 3 ARTICLE 2 : CHALLENGES RELATED TO EMERGING RISK MANAGEMENT 28

3.1 Mise en contexte et présentation de l'article 28

3.2 Abstract 29

3.3 Introduction 29

3.4 Risk and RM: The traditional context 31

3.4.1 Traditional risk: A concept based on the exact sciences 31

3.4.2 RM: A process adapted to the traditional risk context 32

3.5 Emerging risk: Change of context, change of paradigm 34

3.5.1 Emerging risk: A concept based on uncertainty 34

3.5.2 Challenges related to emerging RM 38

3.6 IRM: A more strategic, cross-cutting approach to managing risks 41

3.6.1 What is IRM? 41

3.6.2 Governance: The key element of IRM 42

3.6.3 Social constructivism: From multidisciplinarity to transdisciplinarity, reducing risks by increasing collective knowledge 45

3.7 Discussion and conclusion....47

CHAPITRE 4 MÉTHODOLOGIE DE RECHERCHE 50

4.1 Hypothèses et question de recherche....50

4.2 Objectifs de recherche 53

4.2.1 Objectif général 53

4.2.2 Objectifs spécifiques 54

4.3 Méthodologie de recherche 59

4.3.1 Fonctionnement général de la recherche 59

4.3.2 Méthodologie de recherche 61

CHAPITRE 5 REVUE DE LA LITTÉRATURE 69

5.1 Les outils....70

5.2 Les normes et les standards 71

5.3 Les cadres de gestion des risques 73

5.3.1 L'*Enterprise risk management framework* du COSO....74

5.3.2 Le *Risk governance framework* de l'IRGC 83

5.3.3 Le *Cybersecurity framework v2.0* du NIST 93

5.3.4 Le *COBIT framework for information technology management and governance* de l'ISACA 99

5.4 Les politiques, les guides et les lignes directrices 112

5.4.1 Le Guide de gestion intégrée du risque du Gouvernement du Canada 112

5.4.2 Le Modèle de politique en GIR du Gouvernement du Québec....116

5.4.3 Les Lignes directrices sur la GIR de l'Autorité des Marchés Financiers (AMF) ..119

5.5 Analyse critique....122

CHAPITRE 6 ARTICLE 3 : A GOVERNANCE FRAMEWORK FOR ACHIEVING TRANSVERSAL AND STRATEGIC INTEGRATION OF RISK MANAGEMENT IN LARGE ORGANIZATIONS 128

6.1 Mise en contexte et présentation de l'article 128

6.2 Abstract 132

6.3 Introduction 132

6.3.1 IRM: A summary description 132

6.3.2 The complexity of IRM in large organizations 133

6.3.3 The twofold integration challenge of IRM 135

6.4 The SMM: Achieving the goal of transversal integration of IRM 136

6.4.1 The aggregation model 137

6.4.2 The program charters 139

6.4.3 The MCMs governance matrix 141

6.5 The CFR: Achieving the goal of strategic integration of IRM 143

6.5.1 The policies and directives 144

6.5.2 The processes 145

6.5.3 The standards 146

6.5.4 The key performance indicators (KPIs) 147

6.5.5 The OUs governance matrix 148

6.6 The overall representation of IRM-related governance 150

6.7 Discussion and conclusion 151

CHAPITRE 7 ARTICLE 4 : A COOPERATIVE STRUCTURE FOR INTEGRATED RISK MANAGEMENT IN LARGE ORGANIZATIONS 154

7.1 Mise en contexte et présentation de l'article 154

7.2 Abstract 160

7.3 Introduction 161

7.4 The functional structure of large organizations: An issue for IRM.....162

7.5 The cooperative structure: enabling strategic and crosscutting integration of risk-related activities 167

7.5.1 The 3LoD model and the concept of UE.....167

7.5.2 The cooperative structure 169

7.6 Discussion and conclusion.....175

CHAPITRE 8 ARTICLE 5 : A KNOWLEDGE-BASED RISK-DATA AGGREGATION MODEL LEVERAGING SOCIAL CONSTRUCTIVISM AND SHARED SITUATIONAL AWARENESS TO IMPROVE DECISION-MAKING IN LARGE ORGANIZATIONS 176

8.1 Mise en contexte et présentation de l'article 176

8.2 Abstract.....180

8.3 Introduction 181

8.4 What is SSA?.....183

8.5 The aggregation model 184

8.6 SMM: From risk perception to risk representation 187

8.7 The COF: From risk representation to projection of anticipated situations 193

8.8 Discussion and conclusion.....196

CHAPITRE 9 DISCUSSION GÉNÉRALE 198

9.1 Synthèse des travaux 198

9.2 Apports scientifiques de la recherche.....205

9.3 Limites de la recherche et perspectives de projets 208

CHAPITRE 10 CONCLUSION..... 215

RÉFÉRENCES..... 218

LISTE DES TABLEAUX

Tableau 5.1 Les cinq composantes de l'*Enterprise risk management framework* (COSO, 2017) 75

Tableau 5.2 Décomposition des principes 1 et 2 de l'*Enterprise risk management framework* (COSO, 2017)..... 76

Tableau 5.3 Caractérisation des environnements interne et externe de l'organisation selon le COSO (COSO, 2017)..... 77

Tableau 5.4 Objectifs d'affaires, mesures de performance et cibles selon le COSO (COSO, 2017) 78

Tableau 5.5 Analyse de risques pour deux objectifs d'affaires selon le COSO (COSO, 2017) ... 79

Tableau 5.6 Décomposition du principe 19 de l'*Enterprise risk management framework* (COSO, 2017)..... 81

Tableau 5.7 Décomposition du principe 20 de l'*Enterprise risk management framework* (COSO, 2017)..... 82

Tableau 5.8 Les cinq composantes du *Risk governance framework* (IRGC, 2017)..... 85

Tableau 5.9 Type de risques et caractérisation des connaissances (IRGC, 2017) 87

Tableau 5.10 Stratégies de gestion recommandées par l'IRGC en fonction du type de risque (IRGC, 2017)..... 89

Tableau 5.11 Les déficits de gouvernance potentiels selon l'IRGC (IRGC, 2017) 90

Tableau 5.12 Les six fonctions du cadre NIST (NIST, 2024)..... 94

Tableau 5.13 Catégories associées aux fonctions du cadre NIST (NIST, 2024) 95

Tableau 5.14 Décomposition des catégories GV.OC et GV.RM du cadre NIST (NIST, 2024)... 96

Tableau 5.15 Niveaux de maturité proposés par le NIST (NIST, 2024)..... 96

Tableau 5.16 Fiche relative à l'objectif EDM03 – *Ensured risk optimization* (ISACA, 2018b) 102

Tableau 5.17 Objectifs d'entreprise et objectifs d'alignement selon COBIT 2019 (ISACA, 2018b) 102

Tableau 5.18 Fiche relative au processus EDM03.01 – Evaluate risk management (ISACA, 2018b) 104

Tableau 5.19 Fiche relative à la composante « structures organisationnelles » de l'objectif EDM03 (ISACA, 2018b) 105

Tableau 5.20 Les 33 rôles (acteurs) prédéfinis dans COBIT 2019 (ISACA, 2018b) 106

Tableau 5.21 Fiche relative à la composante « flux d'information » de l'objectif EDM03 (ISACA, 2018b)..... 107

Tableau 5.22 Fiche relative à la composante « politiques et procédures » de l'objectif EDM03 (ISACA, 2018b) 108

Tableau 5.23 Fiche relative à la composante « culture, éthique et comportement » de l'objectif EDM03 (ISACA, 2018b) 108

Tableau 5.24 Fiche relative à la composante « personne, habiletés et compétences » de l'objectif EDM03 (ISACA, 2018b) 108

Tableau 5.25 Fiche relative à la composante « services, infrastructure et applications » de l'objectif EDM03 (ISACA, 2018b) 108

Tableau 5.26 Processus EDM03.01 – *Evaluate risk management* du cadre COBIT (ISACA, 2018b) 109

Tableau 5.27 Processus APO12.02 – *Analyze risk* du cadre COBIT (ISACA, 2018b) 110

Tableau 5.28 Processus APO12.06 – *Respond to risk* du cadre COBIT (ISACA, 2018b) 111

Tableau 5.29 Les neuf principes du cadre de GIR du Gouvernement du Canada (Gouvernement du Canada, 2016)..... 112

Tableau 5.30 Rôles et responsabilités des différents groupes selon le cadre de GIR du Gouvernement du Canada (Gouvernement du Canada, 2016)..... 114

Tableau 5.31 Étapes recommandées par le cadre de GIR du Gouvernement du Canada (Gouvernement du Canada, 2016) 115

Tableau 5.32 Les huit principes directeurs du cadre de GIR du Gouvernement du Québec (Gouvernement du Québec, 2022) 117

Tableau 5.33 Les quatre phases du cycle de gestion du cadre de GIR du Gouvernement du Québec (Gouvernement du Québec, 2022) 117

Tableau 5.34 Rôles et responsabilités des différents groupes selon le cadre de GIR du Gouvernement du Québec (Gouvernement du Québec, 2022) 118

Tableau 5.35 Les quatre principes directeurs du cadre de GIR de l'AMF (AMF, 2015) 119

Tableau 5.36 Rôles et responsabilités des différents groupes selon le cadre de GIR de l'AMF (AMF, 2015)..... 120

Tableau 6.1 MCMs governance matrix (partial)..... 142

Tableau 6.2 OUs governance matrix..... 148

Tableau 8.1 MCMs vulnerabilities matrix (partial) 190

LISTE DES FIGURES

Figure 2.1 Representation of a CS (Robert et al., 2007) 12

Figure 2.2 Dependency curves and supply zone associated with equipment X..... 13

Figure 2.3 Simulation of a DE by DOMINO (t = 0 h) 14

Figure 2.4 Simulation of a DE by DOMINO (t = 4 h) 15

Figure 2.5 Simulation of a domino effect by DOMINO (t = 7h) 16

Figure 3.1 ISO RM process (ISO, 2018)..... 33

Figure 3.2 Typical risk heat map..... 34

Figure 3.3 Key elements of governance..... 44

Figure 3.4 Illustration of the transition from traditional RM to IRM 48

Figure 4.1 Analogie entre les IC d'un environnement socio-économique et les UF d'une grande organisation 52

Figure 4.2 Représentation des interdépendances entre les IC (Rinaldi et al. 2001)..... 55

Figure 4.3 RMC de la problématique des interdépendances entre les IC (Robert et Morabito, 2010b) 55

Figure 4.4 Structure de coopération du projet DOMINO (Morabito et Robert, 2015) 56

Figure 4.5 Exemple d'une courbe d'effet domino (Robert et Morabito, 2010b) 58

Figure 4.6 Cycle de la démarche de la recherche-action (Roy et Prévost, 2013) 63

Figure 5.1 L'*Enterprise risk management framework* du COSO (COSO, 2017) 74

Figure 5.2 Les 20 principes de l'*Enterprise risk management framework* (COSO, 2017)..... 75

Figure 5.3 Différents repères de risques selon le COSO (COSO, 2017) 78

Figure 5.4 Cible et tolérance pour un objectif d'affaires donné selon le COSO (COSO, 2017) .. 79

Figure 5.5 Matrice de risques proposée par le COSO (COSO, 2017) 80

Figure 5.6 Performance réelle vs cible selon le COSO (COSO, 2017) 80

Figure 5.7 Le *Risk governance framework* de l'IRGC (IRGC, 2017) 84

Figure 5.8 Matrice d'évaluation des risques proposée par l'IRGC (IRGC, 2017)..... 88

Figure 5.9 Parties prenantes à impliquer selon le type de risque selon l'IRGC (IRGC, 2017)..... 90

Figure 5.10 Le *Cybersecurity framework v2.0* (NIST, 2024) 93

Figure 5.11 Le *COBIT framework for information technology management and governance* (ISACA, 2018a) 99

Figure 5.12 Les 40 objectifs du cadre COBIT (ISACA, 2018a)..... 101

Figure 5.13 Les sept composantes de la gouvernance selon COBIT 2019 (ISACA, 2018a)..... 103

Figure 5.14 Les six niveaux de maturité des processus considérés par COBIT (ISACA, 2018a) 105

Figure 6.1 Concept de risque basé sur le triptyque aléas/vulnérabilités/impacts (adaptée de Robert et Morabito, 2013)..... 130

Figure 6.2 Proposed IRM aggregation model 138

Figure 6.3 Overview of the risk management ecosystem in large organizations..... 139

Figure 6.4 CFR structure and its elements 144

Figure 6.5 Overall representation of the status of the organization IRM-related governance 150

Figure 7.1 Structure de coopération suggérée pour la GIR..... 155

Figure 7.2 Arrimage de la structure de coopération selon un mode de gestion fonctionnel..... 156

Figure 7.3 Arrimage de la structure de coopération selon un mode de gestion matriciel..... 157

Figure 7.4 Arrimage de la structure de coopération selon un mode de gestion agile et organique 158

Figure 7.5 Arrimage de la structure de coopération selon un mode de gestion hybride (matricielle forte et agile et organique) 159

Figure 7.6 Overview of the roles/responsibilities related to ORM 163

Figure 7.7 Cooperative structure for IRM..... 169

Figure 8.1 Aggregation model based on hazards, vulnerabilities and impacts 185

Figure 8.2 Representation of an MCM's overall condition based on the vulnerabilities affecting the six defined issues 188

Figure 8.3 SMM of the vulnerabilities of Asset 1 193

Figure 8.4 Conceptualisation of aligned vulnerabilities on the Human hazards – Asset 1 – Technological impacts path 195

LISTE DES SIGLES ET ABRÉVIATIONS

3LDD	Trois Lignes de Défense
3LoD	Three Lines of Defence
AGR	Activité liée à la Gestion des Risques
AHP	Analytic Hierarchy Process
AI	Artifical Intelligence
AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
AMF	Autorité des Marchés Financiers
CBA	Consequences-Based Approach
CCPS	Center for Chemical Process Safety
CDSE	Center for Development of Security Excellence
CFR	Common Frame of Reference
CI	Critical Infrastructure
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technologies
COC	Cadre Opérationnel Commun
COP	Common Operational Picture
COSO	Committee of Sponsoring Organizations
CRC	Cadre de Référence Commun
CRP	Centre Risque & Performance
CS	Cooperative Space
DE	Domino Effect
EC	Espace de Coopération
ÉGIR	Équipe de Gestion Intégrée des Risques
ERM	Enterprise Risk Management
GGI	Global Governance Index
GIR	Gestion Intégrée des Risques
GOC	Government of Canada
IA	Intelligence Artificielle
IAA	Institute of Internal Auditors
IAIS	International Association of Insurance Supervisors
IC	Infrastructure Critique
ICII	Informations, Connaissances, Incertitudes et Inconnus
ICP	Indicateur Clé de Performance
ICR	Indicateur Clé de Risque

ICSI	Institut pour une Culture de Sécurité Industrielle
IFMA	International Facility Management Association
IGG	Indice Global de Gouvernance
IGOPP	Institute for Governance of Private and Public Organizations
IAEA	International Atomic Energy Agency
IRGC	International Risk Governance Council
IRM	Integrated Risk Management
IRMT	Integrated Risk Management Team
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISP	Intelligence Situationnelle Partagée
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MAC	Mutual Awareness and Complementarity
MCM	Mitigation and Control Measure
MMC	Mesure de Mitigation et Contrôle
NFPA	National Fire Protection Association
NIMBY	Not In My Back Yard
NIST	National Institute of Standards and Technology
NRC	Natural Resources Canada
OECD	Organization for Economic Co-operation and Development
ORM	Operational Risk Management
OU	Organizational Unit
PMI	Project Management Institute
RACI	Responsible, Accountable, Consulted and Informed
RCCTT	Réseau des Centres Collégiaux de Transfert de Technologie
RDARR	Risk Data Aggregation and Risk Reporting
RM	Risk Management
RMC	Représentation Mentale Commune
RNC	Ressources Naturelles Canada
ROI	Return On Investment
SC	Strategic Community
SMART	Specific, Measurable, Assignable, Realistic and Time-related
SMM	Shared Mental Model
SSA	Shared Situational Awareness
TEPCO	Tokyo Electric Power Company
UE	Unité d’effort / Unity of Effort

UF	Unité Fonctionnelle
UNDRR	United Nations Office for Disaster Risk Reduction
US DHS	United States Department of Homeland Security
US DOD	United States Department of Defense
US DOE	United States Department of Energy

CHAPITRE 1 INTRODUCTION

L'environnement évolue à un rythme effréné. Au même rythme, les risques auxquels sont confrontées les sociétés modernes se modifient et se complexifient largement. Les changements climatiques accroissent la fréquence et l'intensité des phénomènes climatiques extrêmes et bouleversent les environnements et les écosystèmes (United Nations Office for Disaster Risk Reduction [UNDRR], 2019) ; les nouvelles technologies, reposant sur des systèmes de plus en plus intelligents, complexes et interconnectés, donnent naissance à des phénomènes d'effets domino difficilement prévisibles (UNDRR, 2019) ; les réseaux sociaux offrent une tribune inespérée permettant de véhiculer toute forme d'information infondée capable de saper le tissu social ou d'ébranler la confiance des populations envers leurs institutions (European Commission, 2016). Qu'ils soient naturels, technologiques ou humains, les nouveaux risques auxquels sont confrontées les sociétés modernes – et qui sont qualifiés d' « émergents » – créent un environnement hautement dynamique et instable auquel les organisations doivent continuellement s'adapter afin de remplir leur mission et, dans les cas extrêmes, demeurer en vie (Jacob et Michel, 2020).

Les risques émergents sont des risques aux caractérisques particulières qui font en sorte que ceux-ci évoluent à l'extérieur du cadre épistémologique lié aux risques traditionnels. Leur forte incertitude[2] et leur ambiguïté[3] font en sorte qu'il devient de plus en plus difficile de les adresser via les processus usuels de gestion des risques (UNDRR, 2019 ; International Risk Governance Council [IRGC], 2018) ; leur complexité[4], due à l'interaction et l'interdépendance entre les systèmes, et leur propension à se propager de l'un à un autre par le biais d'effets domino difficilement prévisibles font en sorte qu'il devient de plus en plus compliqué pour les organisations de les gérer seules. Pour les gérer de manière plus efficace, des approches de Gestion Intégrée des Risques (GIR) plus globales, multidisciplinaires et multiorganisationnelles deviennent nécessaires (UNDRR, 2015).

---

[2] L'incertitude liée aux risques émergents fait référence à un manque (ou absence) de données scientifiques ou techniques, ou à un manque de clarté ou de qualité de ces données (IRGC, 2018).

[3] L'ambiguïté entourant les risques émergents résulte de perspectives divergentes sur ces risques, y compris la probabilité et la gravité des effets indésirables potentiels (IRGC, 2018).

[4] La complexité liée aux risques émergents naît des difficultés associées à l'identification et à la quantification des causes associées à des effets indésirables spécifiques, ainsi qu'à la compréhension du fonctionnement des systèmes sociotechniques et des interdépendances entre eux (IRGC, 2018).

Une telle approche a été développée par le *Centre risque & performance* (CRP) de Polytechnique Montréal dans le cadre du projet DOMINO, visant à trouver une solution à la problématique des interdépendances entre les Infrastructures Critiques (IC) (Robert et al., 2007). Pour y arriver, le CRP a travaillé avec les principales IC du Québec en mettant sur pied le concept d'Espace de Coopération (EC) (Robert et al., 2007). Reposant sur la mise en commun d'informations ciblées dans un contexte favorable, l'EC est une forme de modèle de coopération dont le fonctionnement est similaire à la communauté stratégique (Kodama 2005a, Kodama 2005b, Kodama 2007)[5]. Le fondement de la communauté stratégique est d'ouvrir la voie à l'échange d'information entre plusieurs organisations concernées par une problématique particulière et commune, mais dont la résolution dépasse le cadre de gestion d'une seule organisation. Ainsi, la réponse à la problématique ne peut être obtenue que par une coopération entre toutes les organisations concernées. Cependant, à la différence de la communauté stratégique, dont le mandat est limité dans le temps, celui de l'EC vise à s'inscrire dans la durée. De plus, le fonctionnement de l'EC repose sur la présence d'un animateur neutre possédant des compétences reconnues dans le domaine concerné par la problématique à résoudre et dont le rôle est d'assurer le lien entre toutes les organisations coopérantes afin de les guider vers une solution qui convienne à toutes (Morabito et Robert, 2015).

Le projet DOMINO a prouvé qu'il existe des gains indéniables que de telles approches de GIR basées sur la coopération peuvent apporter en termes d'accroissement de la connaissance et de la compréhension des risques émergents. Or, ces coopérations se heurtent à la réalité que les organisations y prenant part sont habituées à gérer leurs risques seules (Bharosa et al., 2010). De surcroît, étant structurées de manière fonctionnelle, la majorité des grandes organisations, surtout celles de l'ampleur des IC, gèrent aussi leurs risques de manière fonctionnelle (Chen et al., 2013 ; Jean-Jules et Vicente, 2020). C'est-à-dire que la gestion des risques, au sein de ces grandes organisations, est généralement scindée et répartie entre plusieurs Unités Fonctionnelles (UF) relativement indépendantes, chacune responsable de gérer une Activité liée à la Gestion des

[5] Proposé par Mitsuru Kodama (2005a, 2005b, 2007), le concept de la communauté stratégique est basé sur l'expérience du Nippon Telegraph and Telephone Corporation (NTT Docomo), plus grand opérateur de télécommunications japonais qui, au tournant des années 2000, a réalisé avec succès un vaste programme d'innovation technologique visant à rendre l'Internet accessible via les téléphones mobiles. À cette époque, la migration des réseaux de télécommunications mobiles vers la troisième génération (qui allait permettre d'avoir accès à l'Internet via les téléphones intelligents) présentait une problématique de taille en raison de la multitude de protocoles de communications qui étaient développés par les fournisseurs de service de télécommunications et qui n'étaient pas nécessairement compatibles entre eux. Or, cette problématique dépassait largement le seul cadre de l'entreprise NTT Docomo. L'idée proposée par Kodama, et qui portera ses fruits, consista alors à mettre sur pied un groupe de travail multiorganisationnel dont les membres étaient issus des principales organisations du secteur des télécommunications concernées par la problématique pour trouver une solution qui allait bénéficier à l'ensemble du secteur.

Risques (AGR), comme la continuité des affaires, les mesures d'urgence, la sécurité physique, la sécurité de l'information, la sécurité informatique ou la santé et la sécurité au travail, par exemple. Or, comme ces UF opèrent généralement en vase clos, il n'y a pas nécessairement une coordination de toutes ces activités ou une agrégation des Informations et des Connaissances, mais aussi des Incertitudes et des Inconnus (ICII) sur les risques qui sont réparties à travers ces UF, donc à travers l'organisation (Chionis et al., 2022 ; Jean-Jules et Vicente, 2020 ; Sarker et al., 2016). Or, cette agrégation est absolument essentielle pour permettre à l'organisation d'avoir une vision plus holistique des risques auxquels elle est confrontée, de mieux supporter ses processus de prise de décisions plus tactiques et stratégiques relatifs à leur gestion et de s'assurer que toutes les UF travaillent réellement en synergie (Jean-Jules et Vicente, 2020 ; Chionis et al., 2022). Cela est d'autant plus important dans un contexte où les organisations sont davantage confrontées à des risques émergents ayant la capacité d'affecter transversalement l'organisation (IRGC, 2018).

Les travaux faisant l'objet de cette thèse s'inscrivent dans la continuité de ceux ayant porté sur DOMINO. Ces derniers ont représenté un premier cycle de recherche qui a permis d'élargir les connaissances sur les risques liés aux interdépendances entre les IC et de trouver un moyen de les modéliser. Ce faisant, les travaux ont ouvert sur une problématique nouvelle consistant au maintien sur le long terme d'un EC multiorganisationnel relié à la GIR. À ce sujet, ces travaux suggèrent que pour maintenir efficacement un EC dédié aux risques, un travail en amont doit être réalisé au sein des grandes organisations afin qu'elles-mêmes adoptent des manières plus intégrées de gérer les risques. En effet, il apparaît assez clairement que si l'on veut mettre de l'avant des approches multiorganisationnelles de GIR, encore faut-il que les organisations elles-mêmes adoptent ce genre d'approches. L'objet de cette recherche doctorale est donc d'explorer cette problématique de la GIR au sein des grandes organisations. Plus spécifiquement, elle vise à développer un cadre de gouvernance pour la GIR chez les organisations de grande ampleur.

Pour cela, le prochain chapitre de cette thèse présente un article portant sur les leçons apprises du projet DOMINO. Cet article sert à expliquer le contexte qui a conduit à ces travaux de recherche et ouvre sur la problématique couverte dans cette thèse. Il présente aussi l'hypothèse spécifique qui est à la base de ces travaux de recherche, à savoir que le concept d'EC, qui a permis aux organisations partenaires dans le projet DOMINO d'échanger des informations entre elles dans le but de trouver une solution à la problématique des interdépendances, pourrait être transposé à l'interne des grandes organisations pour prendre la forme d'un cadre de gouvernance pour la GIR.

Cet article a fait l'objet d'une publication dans le *International Journal of Critical Infrastructures* (Morabito et Robert, 2023a).

Le chapitre 3 présente quant à lui un article portant sur les défis liés à la gestion des risques émergents. Cet article se veut une forme de revue de la littérature relative aux notions de risque émergent et de GIR et vise à établir une base de compréhension commune des principaux concepts abordés dans cette thèse. Ainsi, l'article part des concepts traditionnels de risque et de gestion des risques pour introduire les notions de risque émergent et de GIR. Il montre que la GIR est d'abord et avant tout une question de gouvernance et doit être abordée dans une optique d'accroissement de la connaissance collective et de la compréhension de l'organisation des risques auxquels elle est confrontée et de la clarification des rôles et des responsabilités des acteurs organisationnels vis-à-vis de la gestion de ces risques, mettant ainsi de l'avant les deux concepts qui sont au coeur du cadre de gouvernance pour la GIR chez les organisations de grande ampleur qui est proposé dans cette thèse, à savoir, le socioconstructivisme et l'Intelligence Situationnelle Partagée (ISP). Cet article a fait l'objet d'une publication dans le *International Journal of Risk Assessment and Management* (Morabito et Robert, 2023b).

Partant des conclusions issues des publications présentées aux chapitres 2 et 3, le chapitre 4 présente la méthodologie de recherche qui sera employée dans le cadre de ce projet de recherche. Ce chapitre présente donc les hypothèses sous-tendant les travaux de recherche, la question de recherche à laquelle ces travaux tenteront de répondre, les objectifs poursuivis par ces travaux ainsi que la méthodologie qui sera employée pour atteindre ces objectifs et, en définitive, répondre à la question de recherche.

Le chapitre 5 propose quant à lui une revue de la littérature d'éléments d'intérêt liés à la GIR. L'objectif de cette revue est principalement de valider la pertinence de la question de recherche (voire, la réorienter ou la préciser au besoin). Ainsi, après avoir expliqué certains éléments d'intérêt liés à la GIR, une analyse critique de ceux-ci est effectuée. Cette analyse permettra de donner une orientation claire aux travaux de recherche et de mieux apprécier l'originalité du cadre de gouvernance proposé dans cette thèse en regard de l'existant.

Les chapitres 6, 7 et 8 constituent le coeur des travaux de recherche. Chacun de ces chapitres présente un article qui aborde un pilier du cadre de gouvernance pour la GIR chez les organisations de grande ampleur qui est présenté dans cette thèse. Chacun de ces piliers est dérivé d'un élément

caractéristique de l'EC qui avait été mis sur pied dans le cadre du projet DOMINO. Ces piliers sont le référentiel commun, la structure de coopération et le modèle d'agrégation des ICII sur les risques.

Ainsi, le chapitre 6 présente un article qui porte sur le premier pilier du cadre de gouvernance pour la GIR : le référentiel commun. Dans cet article, on montre que la GIR présente un double défi d'intégration : un défi d'intégration horizontal, pour permettre l'arrimage entre les différentes UF au sein de l'organisation, et un défi d'intégration verticale, pour permettre l'arrimage entre les niveaux stratégique, tactique et opérationnel de l'organisation (en lien avec la mission, les objectifs et les opérations de l'organisation). Pour atteindre ces objectifs d'intégration, le référentiel commun repose sur deux composantes : (1) une Représentation Mentale Commune (RMC) des concepts de risque et de GIR, permettant d'atteindre l'objectif d'intégration horizontal de la GIR en clarifiant les rôles et responsabilités des UF responsables des AGR, et (2) un Cadre de Référence Commun (CRC), permettant d'atteindre l'objectif d'intégration vertical de la GIR en enchâssant la GIR à l'intérieur d'un cadre documentaire et réglementaire spécifique. L'article propose également des outils opérationnels pour les grandes organisations afin d'opérationnaliser les intégrations horizontale et verticale de la GIR et d'apprécier globalement l'état de leur gouvernance liée à la GIR. Cet article a été accepté pour publication dans la revue *International Journal of Decision Sciences, Risk and Management*.

Le chapitre 7 présente un article qui porte sur le second pilier du cadre de gouvernance pour la GIR : la structure de coopération. Inspirée de la structure qui avait été mise sur pied dans le cadre du projet DOMINO et intégrant les concepts des Trois Lignes De Défense (3LDD) de l'*Institute of Internal Auditors* (IIA) et d'Unité d'Efforts (UE), la structure de coopération vise à consolider l'atteinte des objectifs d'intégration horizontale et verticale de la GIR en favorisant la mise en commun des ICII sur les risques qui sont réparties à travers l'organisation par la création d'un environnement propice aux échanges et à la réflexion entre des experts provenant des différentes UF responsables des AGR. Pour cela, cette structure de coopération prévoit de centraliser les activités liées à la GIR au niveau d'une équipe multidisciplinaire et transversale compétente (appelée ÉGIR), mais d'en décentraliser les actions vers les acteurs organisationnels concernés au sein des différentes UF responsables des AGR. Cet article a été soumis pour publication dans la revue *International Journal of Decision Sciences, Risk and Management*.

Le chapitre 8 présente quant à lui un article qui porte sur le troisième (et dernier) pilier du cadre de gouvernance pour la GIR : le modèle d'agrégation des ICII sur les risques. Faisant le lien avec le chapitre 3, qui montrait que l'un des défis liés à la gestion des risques émergents tient à la perception qu'ont les acteurs de ces risques, cet article propose de réduire les effets de cette perception en misant sur le développement de l'ISP de ces acteurs. Ainsi, dans cet article, les ICII sur les risques qui sont réparties dans l'organisation sont agrégées afin de permettre aux acteurs concernés de développer une RMC des risques auxquels l'organisation est exposée et d'établir une Cadre Opérationnel Commun (COC) pour leur gestion. La RMC et le COC sont les deux composantes essentielles au développement de l'ISP. Cet article a été soumis pour publication dans la revue *International Journal of Risk Assessment and Management*.

Finalement, les chapitres 9 et 10 viennent conclure cette thèse. Le chapitre 9 présente une synthèse des travaux et montre dans quelle mesure les objectifs poursuivis ont été atteints. Il énonce également les principales limitations de cette recherche et fournit quelques recommandations quant aux perspectives de recherches qu'ouvre ce projet. Pour finir, le chapitre 10 présente la conclusion générale de ces travaux de recherche.

CHAPITRE 2 ARTICLE 1 : SUCCESS FACTORS AND LESSONS LEARNED DURING THE IMPLEMENTATION OF A COOPERATIVE SPACE FOR CRITICAL INFRASTRUCTURES

Morabito, L. et Robert, B. (2023). 'Success factors and lessons learned during the implementation of a cooperative space for critical infrastructures', *Int. J. Critical Infrastructures*, Vol. 19, No. 6, pp.527–543, Publié le 23 octobre 2023.

2.1 Mise en contexte et présentation de l'article

Au tournant des années 2000, le CRP de Polytechnique Montréal a conduit une série de projets de recherche sur les interdépendances entre les IC qui lui ont permis de développer DOMINO : un outil capable de modéliser les interdépendances entre les IC et de simuler les effets domino engendrés par leur défaillance (Robert et al., 2012 ; Robert et al., 2013 ; Robert et Morabito, 2008).

Pour y arriver, le CRP a mis sur pied un EC entre les principales IC présentes à Montréal[6] afin que celles-ci puissent s'échanger des informations pertinentes sur leurs dépendances mutuelles. Les travaux sur DOMINO ont démontré les gains que peuvent procurer de telles coopérations en permettant de générer des connaissances collectives nouvelles qui ne peuvent être obtenues autrement. Ainsi, malgré les nombreux enjeux que soulève le partage d'information entre plusieurs organisations (Arnoux, 2015 ; Bharosa et al., 2010 ; Petrenj et al., 2012 ; Robert et al., 2015), ces travaux ont prouvé qu'il y a une réelle valeur ajoutée à ces coopérations multiorganisationnelles dans le domaine des risques, spécialement lorsque vient le temps d'adresser des problématiques complexes et nouvelles qui dépassent le cadre de fonctionnement d'une seule organisation. En revanche, ces travaux ont aussi montré que le maintien d'un EC entre plusieurs organisations représente un défi particulier, surtout lorsque celui-ci est prévu pour s'inscrire dans la durée.

[6] Les partenaires du CRP dans le projet DOMINO étaient : Bell, Gaz Métro (aujourd'hui Énergir), Hydro-Québec, Société de Transport de Montréal, Ministère des Transports du Québec (aujourd'hui Transports et Mobilité durable Québec) et Ville de Montréal (Centre de sécurité civile et Service de l'eau). Le projet était financé par les partenaires, Polytechnique Montréal, le Conseil de recherches en sciences naturelles et génie (CRSNG) et Protection civile Canada dans le cadre de l'initiative de recherche conjointe sur les interdépendances entre les IC.

L'article présenté ci-après se veut une rétrospective du projet DOMINO et vise à expliquer le contexte ayant conduit aux travaux de recherche présentés dans cette thèse. Ainsi, après avoir expliqué brièvement le concept d'EC, l'article présente certains résultats concrets issus de l'outil DOMINO qui illustrent le potentiel des approches de coopération pour adresser les problématiques complexes et nouvelles, comme les risques émergents. Toutefois, malgré les résultats obtenus, l'article fait état de quelques constats qui semblent expliquer pourquoi l'EC n'a pu progresser davantage, notamment celui qui est à la base des travaux présentés dans cette thèse, à savoir que les grandes organisations ont l'habitude de gérer leurs risques seules. À cet effet, l'article suggère que pour permettre à des initiatives comme DOMINO de s'inscrire dans la durée, un travail en amont doit être réalisé au sein des grandes organisations afin qu'elles-mêmes adoptent des approches plus intégrées de gérer les risques, donc des approches de GIR. À cette fin, l'article suggère qu'il serait possible d'adapter le concept d'EC afin qu'il puisse être transposé à l'interne des grandes organisations pour adresser la problématique de la GIR.

2.2 Abstract

It is largely documented that the exchange of information among critical infrastructures (CIs) is crucial to strategies involving the identification of their interdependencies and increasing their resilience. Based on the experience of the *Centre Risque & Performance*, Polytechnique Montréal (Québec, Canada), this paper presents the outcomes of a 15-year project that led to the development of DOMINO: a tool capable of identifying interdependencies among CIs and simulating potential domino effects (DEs) of their failure. This paper illustrates how multi-organisational collaboration can help solve complex problems and shares lessons learned from the DOMINO initiative, which corroborates several observations documented in the literature. This paper suggests that, in order for effective and long-term collaboration to occur between CIs, not only must there be a sustainable governance framework in place, but upstream works must be conducted within these large organisations to encourage them to adopt, internally, more strategic, transversal and integrated risk management approaches.

Keywords: collaboration; cooperation; critical infrastructures; domino effects; information sharing; integrated risk management; interdependencies; large organisations; knowledge; social constructivism.

Reference to this paper should be made as follows: Morabito, L. and Robert, B. (2023) 'Success factors and lessons learned during the implementation of a cooperative space for critical infrastructures', *Int. J. Critical Infrastructures*, Vol. 19, No. 6, pp.527–543.

2.3 Introduction

2.3.1 Interdependencies among CIs: a source of unpredictable DEs

There are many reasons why critical infrastructures (CIs) fail. On one hand, CIs are particularly likely to be affected by failures due to all sorts of hazards in their environment (Pescaroli and Kelman, 2017; Robert and Morabito, 2010a). On the other hand, CIs are known to operate in a highly complex and dynamic way and to have a nonlinear behaviour (Gheorghe and Schläpfer, 2006). They incorporate multiple interconnected systems forming a very complex system-of-systems (Thacker et al., 2017), whose functioning is generally monitored by very sophisticated and automated algorithms, which adapt the system's responses and configuration in real-time based on demand and many other technical performance parameters (Amin, 2002). The complexity of CIs is increased by the fact that these infrastructures are highly interdependent (Rinaldi et al., 2001). Thus, the failure of one system can quickly propagate to other ones through physical, geographic, logical or cyber interdependencies and thereby create unpredictable DEs affecting several infrastructures over extensive territories (Gheorghe and Schläpfer, 2006; Peerenboom et al., 2002; Robert et al., 2007; Thacker et al., 2017). In this context, beyond 'normal' outages that occur regularly in systems the size of CIs and that are part of their ongoing management, their complexity and their interdependencies mean that all the conditions exist to ensure that any given disaster may assume unsuspected proportions (Thacker et al., 2017). That is why, during events like the blackout of August 2003 in the northeastern USA and Ontario (Natural Resources Canada [NRC] and US Department of Energy [US DOE], 2006) and the one in Europe in November 2006 (European Regulators' Group for Electricity and Gas [ERGEG], 2007; Union for Co-ordination of Transmission of Electricity [UCTE], 2007), a local failure quickly degenerated, affecting very large portions of the territory.

2.3.2 Information sharing: a real challenge for collaborative approaches

DEs are characterised by a spatiotemporal propagation of cascading failures. One infrastructure that fails affects a territory in which other infrastructures are located; they in turn may fail, affecting larger territories and other infrastructures, and so on. Consequently, an analysis of interdependencies among CIs must necessarily combine three parameters: failure, time and space (Robert and Morabito, 2008). The *Centre Risque & Performance* (CRP) has summarised the problematic of interdependencies to the studying of customer/supplier-type relations that link systems. By identifying the resources that systems use and determining how the loss of these resources can affect their functioning (over time and considering possible alternatives), and by delimitating the geographic areas that would be impacted by the failure of these systems, it is possible to identify the consequences, in terms of DEs, of the loss of any given resource or the failure of any given system (Robert and Morabito, 2011).

The major challenge associated with analyses of interdependencies relates to the fact that, to be valid, these analyses require access to information from the CIs themselves. In fact, it is impossible for a single organisation to have all the required resources, information and competence to deal with issues such as interdependencies (Petrenj et al., 2012). This is because it is impossible for one organisation to know what resources other CIs' use and to realistically predict to what degree the loss of these resources will prevent these organisations to deliver their own resources. Hence, to generate reliable and realistic results, studies of interdependencies must absolutely involve people who know how these systems function, namely the managers of the CIs themselves (Robert et al., 2007). However, there are many barriers to information sharing and collaboration (Petrenj et al., 2012) and organisations' confidentiality policies mean that it is very difficult for them to share information with others (Arnoux, 2015; Bharosa et al., 2010; Cho, 2005; Cutter, 2003; Koh et al., 2008; Morabito and Robert, 2015; Robert et al., 2015; Samuel and Spalanzani, 2009). Confidentiality is required for a variety of legitimate reasons (trade secrets, confidential information about employees/customers, vulnerabilities, etc.). Hence, one should not read into these organisations' reluctance to share information any sign of unwillingness to collaborate, but rather a genuine responsibility to keep organisational information secure.

2.4 Cooperative space: a model of collaboration dedicated to exchanges of information among multiple organisations

2.4.1 The cooperative space: an environment that fosters information exchange among Cis

The challenge to be met in studying interdependencies among CIs is ensuring that they can share relevant information so their dependencies can be identified and the potential consequences of their failure, anticipated. This amounts to constructing an appropriate environment within which information can be confidently shared. There are numerous models to choose from when it comes to collaborative initiatives implicating public and private organisations and the literature is indeed very rich on that topic. Depending on the nature and the objectives of the collaboration, the numbers of actors implicated, the length of the collaboration, etc., one model can better serve the purpose than another one (Trucco and Petrenj, 2017). On its end, the CRP developed the concept of cooperative space (CS) (Robert et al., 2007).

The operating principles for the CS are similar to those of strategic communities (Kodama, 2005a). It is a model of multi-organisational collaboration that is directly focused on solving a specific problem that is shared by all the organisations taking part in the CS, but to which the response extends beyond the borders of a single organisation's management. The raison d'être of the CS is to allow the organisations concerned by the problem to directly and jointly participate in resolving it. A CS is lead by a moderator who's role is to manage all the aspects of the collaboration and the communication between the CIs. Each organisation in the CS is represented by experts (one, two or more depending on the organisation) that are responsible for providing the information that is required to realise the analysis for which the CS was setup for and for making the link between the works done by the CS and their respective organisation. Figure 2.1 illustrates a representation of a CS setup to analyse interdependencies among CIs.

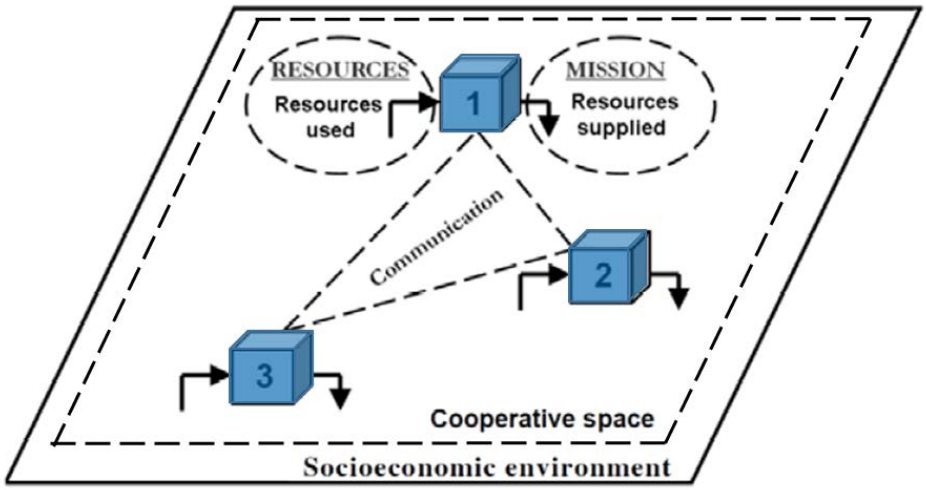


Figure 2.1 Representation of a CS (Robert et al., 2007)

When it comes to studying interdependencies between CIs, the information that is exchanged between organisations is linked to the resources that are being utilised and supplied. The functioning of the CS provides that all organisations remain the sole owners of their information and they alone are responsible for conducting their analyses of internal vulnerability towards the resources they use. Ultimately, only the results of these analyses are shared with the other members of the CS in the form of dependency curves associated with supply zones (Figure 2.2).

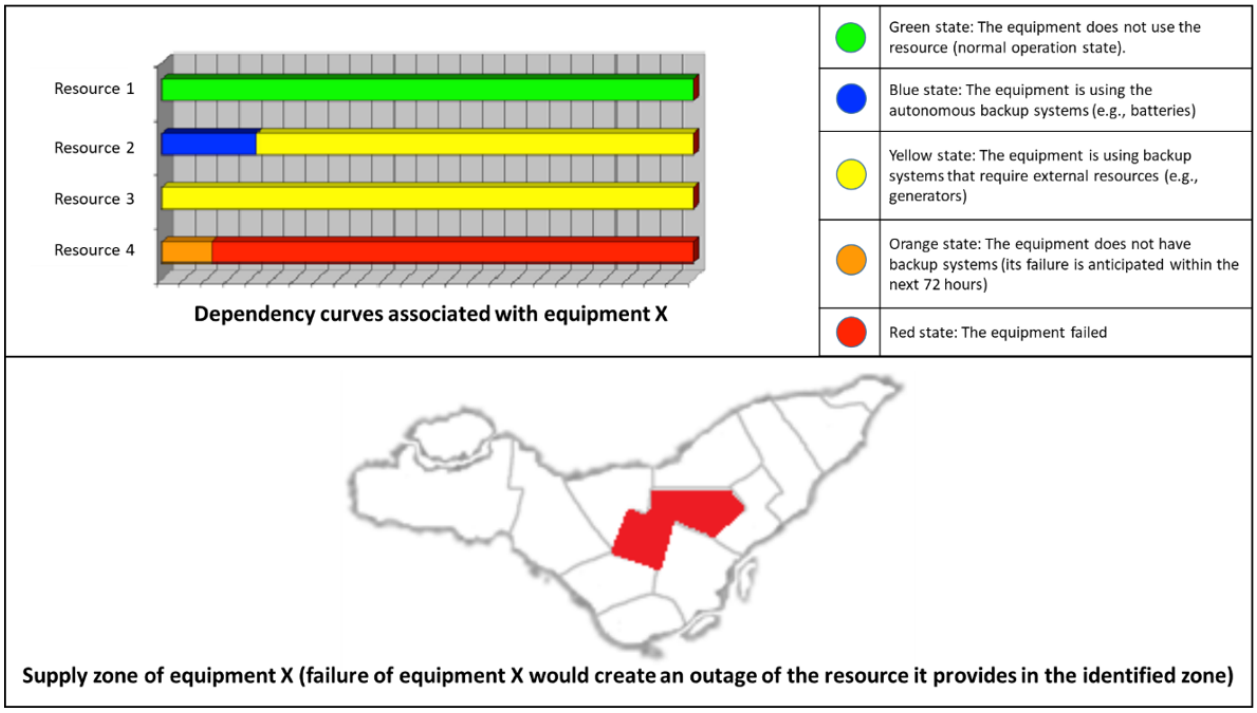


Figure 2.2 Dependency curves and supply zone associated with equipment X

Dependency curves for a given equipment reveal how long this equipment can continue functioning in the absence of the resources it uses. The associated supply zone makes it possible to determine which part of the territory will be impacted by the equipment's failure (in terms of the supply of the resource) (Robert and Morabito, 2008; Robert et al., 2008, Robert et al., 2013). All this information can then be integrated into a tool that makes is possible to determine what DEs may be generated by the failure of any given equipment belonging to any CI, regardless the circumstances/causes that led to the failure.

2.4.2 DOMINO: A Des simulation tool resulting from the works of the Québec CS

DOMINO, which was developed by the CRP as a result of its collaboration with some dozen public and private-sector partners, is the tangible outcome of the works of the CS setup in Québec. It is an expert system that combines a database, a calculation algorithm and a geomatics interface capable of modelling interdependencies among CIs and simulates the DEs triggered by their failure. Using the information that is contained in the dependency curves, DOMINO can generate the chain of potential DEs generated by any given situation affecting any given geographic area or equipment

belonging to a CI, without relying on pre-established failure scenarios. A spatiotemporal animation (temporal cursor) on a geographic support allows users to understand the series of undesirable events occurring over time (Robert et al., 2012).

Figures 2.3 to 2.5 hereafter present an example of simulation realised by DOMINO. Figure 2.3 shows the instant t = 0 h of a simulation of the DEs occurring following the failure of an asset belonging to a CI (equipment noted by the red dot on the map).

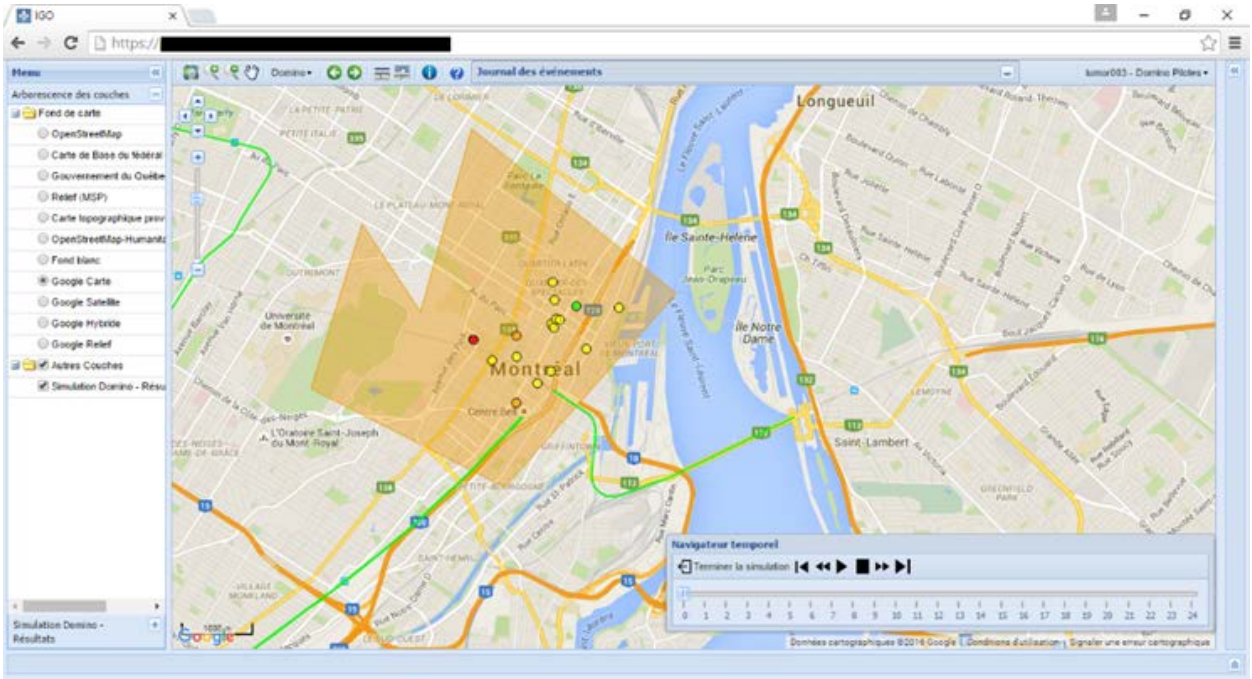


Figure 2.3 Simulation of a DE by DOMINO (t = 0 h)

The shaded area is the one deprived of the resource in question. In this area are located several assets belonging to other CIs. Those represented by a green dot will continue to operate normally since they are not using the resource in question. Those in yellow are affected by the failure of the resource, but continue to operate thanks to means of protection or alternate resources. Those in orange do not have sufficient backup measures and may fail if the situation is not restored, causing a potential DE.

Figure 2.4 represents the situation after four hours.

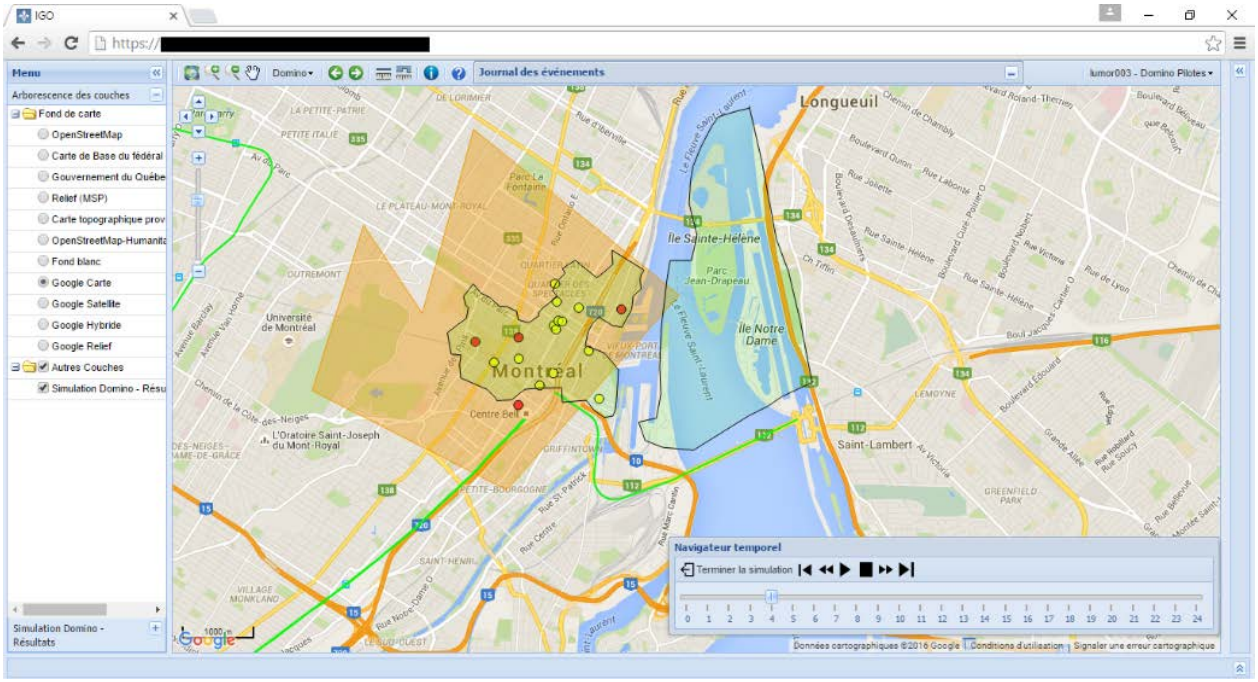


Figure 2.4 Simulation of a DE by DOMINO (t = 4 h)

At the instant t = 4 h, we notice that the two assets which were in the ‘orange’ state at the moment t = 0 h have just moved up to the ‘red’ state and that two other areas have just been deprived from the resources provided by these two assets. In the new impact zones, we notice that an asset belonging to a CI has also failed (red state). By continuing the simulation, we notice that the failure of this asset causes the loss of service of the passenger train after three additional hours, i.e., seven hours after the initial failure, and affects a much larger area (Figure 2.5).

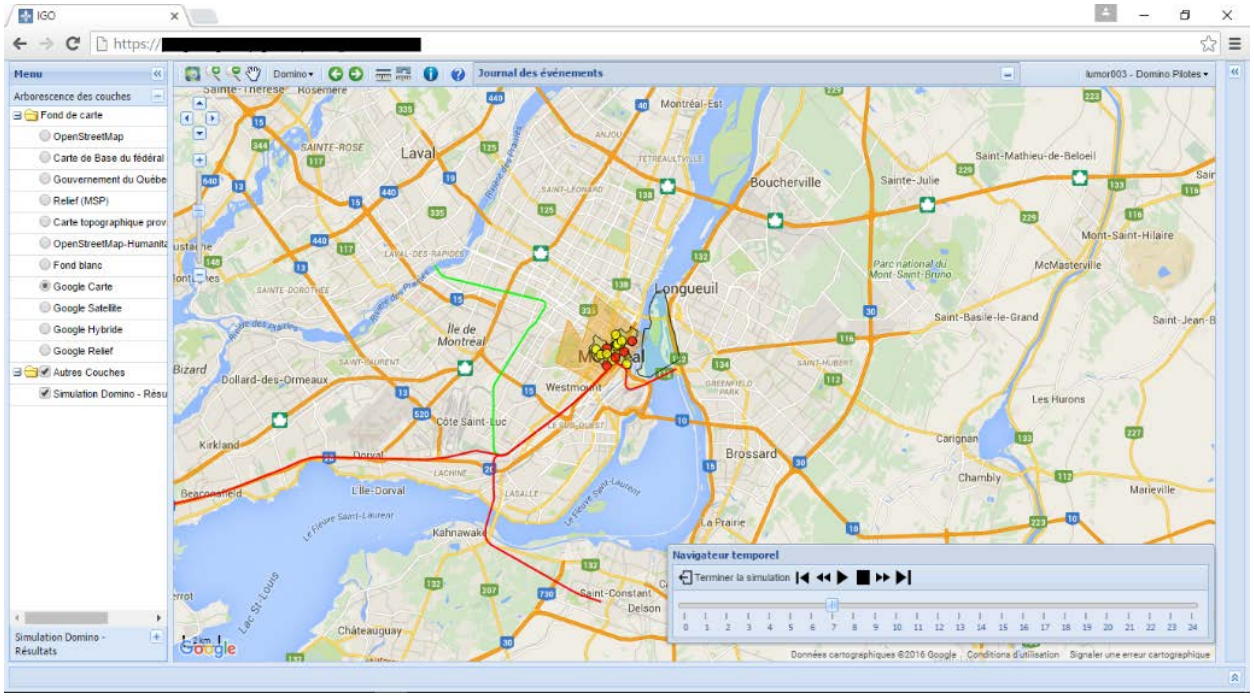


Figure 2.5 Simulation of a domino effect by DOMINO (t = 7h)

The potential of a tool like DOMINO is interesting. For CIs managers and emergency preparedness authorities, the cross-cutting information enables them to better structure their operational and strategic decision-making. At the operational level, simulations make it possible to predict which actions should be taken in priority and which people should be contacted and mobilized to ensure an appropriate, rapid and, above all, concerted and coherent response on the part of all the organizations involved in the situation. For example, the tool has already been used in drills to simulate the DEs generated by explosions related to the transportation of hazardous materials and problems associated with land-use planning (Delvosalle et al., 2017; Robert et al., 2014). It has also been used in a real-life situation to help assess the needs for bottled water during a major boil water advisory in Montreal on May 13, 2013 (Morabito and Lagacé-Banville, 2013). Other simulations related to infrastructures' dependency on electricity, for example, revealed that a large-scale, long-lasting power outage could quickly result in a shortage of fuel for generators, resulting in large-scale DEs. From a strategic perspective, it is then possible to prioritize fuel supplies among organizations in order to minimize adverse consequences (Robert and Morabito, 2009). Other simulations were carried out to assess the dependency of drinking water infrastructures in order to help prioritize the refurbishment of Montreal's water mains by integrating an additional parameter related to the consequences of a failure of those infrastructures (CRP, 2013).

At a more strategic level, the results produced by DOMINO and the increased knowledge of the territory may guide high-level decision-making to increase the resilience of CIs. For instance, several of the CRP's partners have stated that the information contained in the dependency curves gave them more influence with their senior executives when they had to justify investments or actions to guard against certain risks. Analyses can also determine the locations that should be avoided and those that should be favored for the installation of back-up systems (redundancy) – to ensure that the backup systems are not impacted by the same hazards as the equipment from which they must take over in the event of a problem – or for the deployment of new systems/equipment (Robert et al., 2019).

2.5 Success factors associated with the implementation of a CS

The implementation of a CS involving multiple organisations demands a great deal of preparation. In Québec, the CS setup by the CRP was composed of about a dozen organisations from the sectors of drinking water treatment and supply, energy (electricity and natural gas), telecommunications, road transportation, public transit, emergency preparedness, and governments (municipal, provincial and federal). Getting all these organisations to agree on a model for exchanging information was no small matter and the margin of error was low. The CRP has identified three main success factors for the implementation of a CS: the existence of a clear mandate, the presence of a competent moderator, and the adoption of an approach that is respectful of organisations' constraints.

2.5.1 A clear mandate resulting from a real problem

No organisation whatever is willing to share information with another organisation unless it has a specific reason for doing so and it has obtained an authorisation stipulating the terms and conditions of these exchanges (Roy et al., 2011). Thus, the first success factor for implementing a CS is the existence of a clear and solid mandate that unites all the stakeholders. To be clear, the mandate must not allow for any ambiguity about the objective of the collaboration; to be solid, the mandate must be based on the existence of a problem that is real, is shared by all the organisations involved in the collaboration, and most of all, deserves to have time and energy spent on it.

The search for a mandate must be directed by one entity we could call the enabler. The enabler will launch the process of creating the mandate, since it will probably not start spontaneously. Note: not just anyone can be an enabler. The enabler must not only have an excellent understanding of the problem experienced by the organisations taking part in the collaboration but must also have a certain standing in its environment (profile) so it can accrue the necessary authority to convince the target organisations to take part in the collaboration and thereby trigger the process of creating the mandate.

The mandate must legitimise the sharing of information among the organisations by establishing the objectives of these exchanges, the expected outcomes, the types of information to be exchanged, and the measures that will be adopted to secure it. To do this, it is important for the organisations to share a joint strategic vision of the short, medium and long-term objectives. This kind of shared strategic vision is difficult to achieve; however, once established, it justifies the existence of the mandate and ensures they will all work towards achieving the same end-goal. In turn, the mandate justifies the allocation of resources (e.g., human, financial, information) by the organisations involved in the collaboration. This investment of resources is not only necessary for carrying out the studies of interdependencies but also speaks to the seriousness of the problem in the organisations' view and their commitment to the process of exchanging information (Doz and Hamel, 1998; Roy et al., 2012; Vézina and Messier, 2009). The lack of a mandate is a major hindrance to information sharing among organisations (Arnoux, 2015; Morabito and Robert, 2015; Robert et al., 2015). It is therefore crucial to obtain one in order to formalise the creation of a CS. Then, the signing of commitment and confidentiality agreements confirms the mandate.

In the course of the CRP's works, the mandate arose from a Government of Canada funding program that was setup to increase knowledge of interdependencies among CIs. The mandate's enabler was the CRP, which then had to persuade the managers of CIs in Québec to participate in the project. It took almost two years to establish the details of the collaboration.

2.5.2 A competent moderator with demonstrated leadership skills

The second success factor for setting-up a CS is the presence of a moderator whose role is to facilitate collaboration and execute tasks related to the logistics of the collaboration (meetings planning, project schedule, delivery of results, etc.). The moderator's presence within the CS is crucial. Its main role is to ensure that the CS's efforts continue to be focused on the specific

objectives it seeks to achieve and for which it was created. The moderator function is usually adopted by the entity that launched the mandate, namely the enabler, but it may also be accepted by any entity designated by the organisations participating in the CS (e.g., an emergency preparedness authority, a research centre, etc.). The moderator may also appoint expert advisors who can perform certain technical analysis related to the CS's works.

The moderator constitutes the connecting dot between all the organisations taking part in the collaboration. Thus, it is very important to choose it judiciously. Because it will inevitably have access to privileged information coming from the CIs, one of the fundamental criteria for selecting a moderator is that it must be neutral. The moderator must never make individual use of the privileged information it may have to handle or use it for other purposes than those agreed upon in its mandate (Davel and Tremblay, 2006). Since the moderator is the entity on which all the CS members rely for carrying out studies, another important selection criterion is that it must have sufficient knowledge and experience with the problems and issues related to the execution of the mandate, the goals to be achieved, and above all, the means of doing so. Finally, the moderator must possess the necessary interpersonal and relational qualities to fully exercise its role as a catalyst (unifier) for the other CS members. He must demonstrate excellent leadership skills and have a long-term strategic vision in order to keep participants interested (Davel and Tremblay, 2006; Kodama, 2005a; Roy et al., 2012). In the case of the works done in Québec, the moderator was the CRP due to its expertise in the area of risk management.

2.5.3 An approach that respects organisations' confidentiality constraints

The existence of a mandate and the presence of a moderator are not sufficient in themselves to solve the problem the CS was set for. Thus, the third success factor in the implementation of a CS is therefore to adopt a rigorous approach that will make it possible to achieve the objectives of the collaboration while taking into consideration the organisations' confidentiality constraints and their limited capacity to share information. To define this approach, a serious, relatively exhaustive analysis must be done to precisely delineate what the members want to achieve in terms of results, decide on how to do this, and finally, identify the information that will be needed for this purpose and whether the organisations can provide that information. If they cannot, the approach will need to be modified. At this stage, it is very important to adopt an information exchange approach that is flexible enough to ensure compliance with the constraints related to managing the organisations'

confidential information, but specific enough to provide relevant solutions to the problems the CS is trying to solve. The analysis that must be done to determine the ideal approach is therefore crucial. It is not easy to carry out, and may be quite tedious, but it must absolutely not be taken lightly, since all of the CS's subsequent work will depend on it.

In the case of the CRP's works, it took almost three years to develop an approach that fit the CS's operating methods, satisfied all the constraints identified by the partners, and allowed for a satisfactory solution to the problem of identifying interdependencies among them: the consequence-based approach (CBA). The CBA is a risk-management approach that focuses on the consequences associated with the failure of an infrastructure and not on the causes that led to it (Robert and Morabito, 2008; Robert and Morabito 2010a; Robert et al., 2007). Unlike scenarios-based approaches, the CBA relies on the technical analysis of system vulnerabilities to identify situations that are likely to generate DEs. To respect the partners' constraints related to confidential information, all vulnerability analyses are done inside the organisations themselves, while allowing some bipartite (between two organisations) or sectorial discussions (between organisations in the same activity sector) to occur to address specific problems that may affect only the parties in question. One of the advantages of the CBA is that it minimises the information provided by organisations. In addition, by requiring the organisations to do their own analyses, it reduces the possibility of errors related to the misinterpretation of technical data and means that organisations are more inclined to accept the results (Robert and Morabito, 2010a).

2.6 Lessons learned from the DOMINO initiative: the difficulty of maintaining a CS over the long-term

The DOMINO initiative demonstrated the potential of collaborative approaches to address risks that extend beyond the borders of organisations, such as interdependencies. Nevertheless, several difficulties affect the maintenance of a CS over the long-term. The initiative was an opportunity for learning certain lessons and corroborating information found in the literature.

2.6.1 A sustainable governance structure

The first lesson learned from the DOMINO initiative is the importance of implementing a clear governance structure for the CS's operations. Although organisations may invest in a research

project for a limited period, they cannot do so indefinitely unless a sustainable governance structure (explaining the operations and financing of the CS) is in place. The governance structure must clearly indicate who is responsible for the mandate, who will act as moderator, and what organisations are involved. The governance structure must also specify the mission, vision and objectives for the collaboration and the roles and responsibilities of the parties involved.

In the case of the CRP's works, the mandate in which the organisations were involved was a research project to develop a methodology and a tool to analyse interdependencies among them. Their collaboration lasted for almost 15 years, and the mandate was completed successfully. However, the mandate did not provide for the long-term maintenance of the CS and none of the partners had undertaken to extend the mandate indefinitely or even to take over from the CRP and act as moderator once the work was completed. In addition, no specific work had been initiated with the objective of defining a governance structure for the long-term maintenance of the CS. Thus, once the work was complete, the CS could not be kept going.

Regarding the mandate to maintain the CS, the important question is: who should have assigned such a mandate? This question is important since it is related to the identification of the entity that should have assumed the leadership of the CS's governance. In our experience, the question is not really which entity should assume such a role but which one would be willing to assume it. Given its long-term nature, it seems that a government entity responsible for public safety would be the best choice to take over this role since, to some degree, these are the authorities responsible for protecting the public from the consequences of CIs failures. The question then is: which level of government (municipal, provincial or national) should assume the role? At the national level, these problems are viewed more macroscopically, whereas at the municipal level, the problems to be addressed should be much more precise and targeted. Further studies would be required to define the ideal governance structure. Perhaps, a multi-scale public-private partnership governance model based on the functioning of the CS could align local and global issues into one single framework and offer the most benefits.

2.6.2 Ongoing results to keep participants interested

Another lesson learned from the DOMINO initiative is related to the maintenance of the collaborating organisations' interest in the work being done. In fact, it is very difficult in a project like DOMINO (research and development project) to keep organisations interested, since a

significant amount of time may elapse before the CS can provide its end-result. For this reason, it is important for the CS to deliver results, even small ones (quick wins), on an ongoing basis, rather than focusing on delivering one greater final outcome. Indeed, the challenge of keeping participants interested is related to the CS's capacity not only to demonstrate the benefits of the collaborative approach throughout the collaboration process but also, and most importantly, to go beyond the targeted objectives. Once tools have been developed and major interdependencies identified and addressed, organisations have the impression that their work is done. But, the tools themselves represent very little compared to the real gains that a CS can generate over the long-term. The environment, organisations, systems and technologies change, and so do people. Thus, organisations must continue to prepare collectively to handle any disasters. It is therefore important for activities (drills, vulnerability analyses, information updates, upgrades of operational tools, integration of new problems, etc.) to be carried out to maintain organisations' interest and thereby ensure that the collaboration lasts. Consequently, in keeping the CS active and interest levels high, one must also remember that every organisation has its own challenges, problems to solve and objectives to achieve. The challenge then is to make sure that it will be possible to respond to these individual needs while ensuring that this is not done to the detriment of the CS's collective goals. Thus, there is a fair balance to be maintained between collective and individual goals so that all participants are satisfied.

2.6.3 Trust based on the creation of a win-win context

The search for a fair balance between collective and individual objectives highlights another lesson learned from the DOMINO initiative that is well documented in the literature: the importance of mutual trust and the creation of a win-win context (Garrido-Pelaz et al., 2016). As found in Trucco and Petrenj (2017), it was highlighted in a 2012 report from the USA National Infrastructure Advisory Council, following an extensive analysis, that trust was the bonding agent between actors in a collaboration framework. As a matter of fact, in any kind of sharing, a certain distrust naturally tends to set in and represents a major hindrance to collaboration (Doz and Hamel, 1998). The difficulty here lies in ensuring a balance between the information requested and its contribution to the achievement of the CS's collective goals. To this end, the exchange of information must never create (or seem to create) a situation in which one organisation is trying to enrich itself at the expense of others (by gaining access to the other organisations' information) (Doz and Hamel,

1998). That is why a collaborative effort should always ensure that entities that are present only to benefit from others are avoided (Garrido-Pelaz et al., 2016). If that happens, organisations may become distrustful, which would not only be counterproductive, but might even lead to the end of the collaboration.

This contradiction between trust and mistrust related to the social and cognitive dimensions of collaboration must be appropriately managed (Doz and Hamel, 1998). In reality, organisations are very complex socio-technical systems: although part of their operation is purely technical, another part is purely social (Petrenj et al., 2012). It is not easy to create a climate of trust and a win-win context. These are built over time and must be continuously tended since the people within organisations constantly change. Nevertheless, once this atmosphere exists, successful information sharing can almost be guaranteed. For this reason, trust must be supported by tangible means (e.g., confidentiality agreements) to protect information and its use but also by implementing mechanisms that encourage social interactions, since such interactions are what really build trust. From this point of view, the moderator must inspire trust and must never resort to other sources than the partner organisations to obtain information about them. That could seriously damage, or even permanently destroy, the bond of trust.

2.6.4 Measurable gains for the collaborating organisations

Another important lesson from the DOMINO project is the importance of continuously promoting the gains the collaboration creates. Indeed, despite the clear benefits, neither private nor public organisations are prone to collaborate unless there are tangible incentives that motivate them to do it (Garrido-Pelaz et al., 2016). The process of collecting, analysing and exchanging information takes time and resources, so there is a cost associated with it. In addition, the information that is shared possesses intrinsic value. Finally, information sharing represents a certain risk for organisations that is not necessarily quantifiable but that constitutes an additional cost. This investment in time, resources and information, which the organisations agree to make, implies de facto that there must be a return on their investment (Arnoux, 2015; Koh et al., 2008; Morabito and Robert, 2015; Robert et al., 2015). To ensure the sustainability of the CS, it is therefore very important that ultimately the gain related to collaboration [cost-benefit ratio or return on investment (ROI)] is interesting to the participating organisations (Garrido-Pelaz et al., 2016).

The first way of making the cost-benefit ratio interesting is to reduce the cost of collaborating. This amounts to minimising the information being exchanged and the investment of the human resources' time. Interorganisational collaborations are usually entered into voluntarily (Cook and Friend, 1991). Consequently, it is important for the process of exchanging information to be neither too burdensome, nor too demanding, nor coercive in any way. To this end, the process must minimise the information requested from organisations by focusing only on information that can be shared and that is relevant. It must also offer flexibility with reasonable, adaptable milestones, and accept that organisations will not all advance at the same pace.

The other way of making the cost-benefit ratio interesting is to increase the benefit of collaborating. An organisation that shares information with others will legitimately expect to receive in return some value-added information that will enable it to make certain decisions that will have positive impacts. The people who approve the exchange of information must therefore see the advantages of this sharing in the form of the possibility of reaping benefits (e.g., financial, operational or image-related) or avoiding costs (e.g., optimisation of a task, mitigation of a risk, etc.). Thus, in order for the collaboration to be worthwhile and to last for a long time, it must give the participating organisations tangible benefits that they would not otherwise be able to achieve (collective learning) (Dyer and Singh, 1998; Morabito and Robert, 2015; Samuel and Spalanzani, 2009; Vézina and Messier, 2009).

During the works done in Québec, the greatest benefit emphasised by the members of the CS (and probably the least tangible) was that they got to know each other and were able to interact away from real-world situations that forced them to do so. Several partners stated that managing emergencies with people they already knew undoubtedly represented an advantage. Another gain was the access to DOMINO, which is meant to be a real platform for pooling interorganisational information. The simulations can reveal unsuspected vulnerabilities that can then be dealt with during drills dedicated to align emergency plans and ensure coherence. Such coherence is essential since most organisations' business continuity plans rely on the same alternative resources (e.g., fuel for generators in situation of electricity outage, bottled water in situation of water outage). Although these continuity plans work well when considered individually, these alternative resources (fuel, bottled water) could quickly run out when considering the cumulative needs, thus raising important questions regarding their allocation. The alignment of continuity plans makes it possible to prioritise collective action based on the specific situation in order to ensure a

coordinated, coherent response and thus save valuable time during a real-life intervention. It is well known that, in an emergency, the first few minutes are key. Having the right information on hand and being in touch with the right people to make the right decisions at the right time can make the difference between a successful operation and a full-fledged crisis.

Prior knowledge of interdependencies and the propagation of DEs make it possible to reap important benefits, which must be highlighted since they are usually hard to quantify in monetary terms. One of the biggest difficulties related to the quantification of ROI stems from the fact that, in most organisations, risk management is seen as an activity that generates an expense for the organisation. Although it is easy for an organisation to calculate how much it costs to mitigate risks, it is very difficult to estimate the costs avoided due to sound risk management practices (risk management expenses show up in the expense column in the financial statements, whereas costs avoided due to sound risk management are invisible). So it is very important to make sure that risk management in organisations is perceived as a highly strategic, value-generating activity. Likewise, it is very important to the long-term sustainability of a CS to highlight the positive spinoffs and benefits associated with it and strive to link them to metrics or performance indicators that are directly in line with the participating organisations' missions and strategic visions, thereby enabling their management to appreciate their ROI.

2.7 Discussion and conclusion

The growing digitisation of our modern societies and the increasing complexity of CIs and their interdependencies mean that it will become more and more difficult for organisations to manage their risks in silos. Climate change and other natural threats will only exacerbate this difficulty. The COVID-19 crisis is an eloquent example of this trend.

As it is largely documented in the literature, partnerships are the way to go to address CIs protection and resilience. And, the works done by the CRP proved that collaborative approaches to handling risks have a great potential for solving problems that transcend organisational boundaries and can provide very operational results. Nevertheless, the general finding from the works on DOMINO is that it is very difficult to maintain a CS over time when all the conditions required for its sustainability are not met, that is to say, when a clear and structured governance framework is not in place. Obtaining a clear mandate and identifying a long-term moderator are two sine qua none

conditions for maintaining a CS and must be part of the development of a viable long-term governance model. Another condition that is essential for the sustainability of the CS is related to keeping the collaborating organisations interested and highlighting the gains that long-term collaboration can bring. Indeed, initiatives like DOMINO have true social constructivist potential. In this sense, these approaches create value for the participating organisations since they make it possible to pool their individual knowledge to generate new collective knowledge that they could not generate individually but they can then reuse individually and collectively. However, collaborative efforts often come up against the reality that the participating organisations are accustomed to managing their risks alone. Moreover, even within their own walls, organisations – especially those of the size of CIs – very rarely manage their risks in an integrated way. Contrary to conventional risk management, which is meant to be highly functional, integrated risk management is a much more strategic and cross-cutting activity (Amansou and Chaouki, 2019). Although it has been documented that traditional hierarchical frameworks based on vertically aligned organisational structures tend to break down when confronted with uncertainty, dynamicity and complexity of risks (Petrenj et al., 2012; Trucco and Petrenj, 2017), large organisations are for the majority structured in silos, and though they all belong to the same company, there is often little communication among the silos. And, even if it does exist, it is not systematically formalised. Silos tend to have their own ways of managing risks and there is very little integration of all the risk-related works done across the organisation.

In light of these findings, it is clear that to allow initiatives like DOMINO, or like any other public-private partnership, to stand the test of time, it is imperative that a clear governance structure must be put in place and that a leader is mandated to manage the collaboration. In our opinion, it would make perfect sense that a government entity takes that role and that policies fostering information sharing and oriented towards increasing the resilience of CIs are established with the CIs operators and put in place for the long term. Another element that seems clear is that in order for large organisations to fully appreciate the benefits of collaborating and to view collaborations as a strategic component of their resilience, upstream works must be conducted within them to make risk management a strategic activity and to adopt, internally, more integrated and transversal risk management approaches.

In this respect, the similarities between the CIs in the DOMINO initiative and large organisations opens up the possibility for creating CSs within such organisations. Indeed, the structure of large

organisations (division into numerous business units/silos) means that – like the CIs in the CS – they behave like relatively isolated, but still interdependent, societies. Thus, the analogy with CIs and their CS directly suggests an avenue for the development and consolidation of collaborative models similar to the CS but this time within large organisations, in order for them to manage risks in an integrated way. Thus, the CS setup by the CRP to analyse interdependencies among CIs could contribute to such initiatives. Some challenges will certainly be similar (development of a single risk model, aggregation of information on risks, etc.), but others, such as the challenges related to the long-term sustainability of the CS or gaining access to certain information and ensuring confidentiality, could be easier to solve. Nevertheless, the gains from implementing a similar approach within large organisations could be substantial and might eventually lead to revive initiatives like DOMINO (perhaps DOMINO 2.0) that can be sustainable.

CHAPITRE 3 ARTICLE 2 : CHALLENGES RELATED TO EMERGING RISK MANAGEMENT

Morabito, L. et Robert, B. (2023). 'Challenges related to emerging risk management', *Int. J. Risk Assessment and Management*, Vol. 26, No. 2, pp.175–195, Publié le 19 mai 2024.

3.1 Mise en contexte et présentation de l'article

La rétrospective du projet DOMINO présentée au chapitre précédent montre que les approches basées sur la coopération et l'accroissement de la connaissance collective offrent un potentiel intéressant lorsque vient le temps d'adresser des problématiques nouvelles et complexes, comme les risques émergents. Elle suggère aussi que pour permettre à des initiatives comme DOMINO de s'inscrire dans la durée, un travail en amont doit être réalisé au sein des grandes organisations afin qu'elles-mêmes adoptent des approches plus intégrées de gérer les risques, donc des approches de GIR. À ce stade, il convient donc de se poser deux questions. La première : que sont les risques émergents et en quoi ceux-ci diffèrent-ils des risques, que l'on pourrait qualifier de « traditionnels », au point de nécessiter une approche de gestion différente ? Et, la deuxième : qu'est-ce que la GIR et en quoi celle-ci diffère-t-elle de la gestion des risques, que l'on pourrait qualifier de « traditionnelle », au point d'être plus adaptée à la gestion des risques émergents ?

L'article présenté ci-après vise à répondre à ces deux questions. En partant des concepts de risque traditionnel et de gestion des risques, l'article présente les risques émergents et les défis liés à leur gestion. Il explique en quoi les caractéristiques de ces risques font en sorte que ceux-ci ne peuvent pas être adressés de la même manière que les risques traditionnels et montre qu'il y a une inadéquation entre les méthodes qui sont couramment employées par les organisations pour gérer les risques, et qui sont généralement basées sur le processus recommandé par la norme ISO31000 de l'*International Organization for Standardization* (ISO, 2018), et les caractéristiques des risques émergents. L'article enchaîne ensuite sur la notion de GIR et explique en quoi celle-ci diffère de la gestion des risques traditionnelle et pourquoi elle est davantage en adéquation avec les défis liés à la gestion des risques émergents. Finalement, l'article montre que la GIR est avant tout une question de gouvernance et doit être abordée dans une optique d'accroissement de la connaissance

collective et de la compréhension de l'organisation des risques auxquels elle est confrontée et de la clarification des rôles et des responsabilités des acteurs organisationnels vis-à-vis de la gestion de ces risques, mettant de l'avant les deux concepts qui sont au coeur du cadre de gouvernance pour la GIR chez les organisations de grande ampleur qui est proposé dans cette thèse, à savoir, le socioconstructivisme et l'ISP.

3.2 Abstract

The literature agrees on the importance of integrated risk management (IRM) to address the challenges posed by emerging risks. However, many organisations that attempt to implement an IRM initiative experience deep frustrations because they simply cannot succeed despite the devotion of energy and resources. Indeed, although the literature is fairly rich on the topic, we find few documents that give practitioners an explanation (neither brief nor comprehensive) of emerging risks, how their management is different from that of traditional risks, or the explicit implications for organisations implementing an IRM initiative. Based on a literature review, the objective of this paper is to fill this gap by providing practitioners with a better understanding of traditional and emerging risks and the differences between them. Building on this understanding, we explain the challenges associated with managing emerging risks and why traditional approaches to risk management (RM) are limited when faced with these challenges.

Keywords: emerging risk; framework; governance; IRM; integrated risk management; social constructivism.

Reference to this paper should be made as follows: Morabito, L. and Robert, B. (2023) 'Challenges related to emerging risk management', *Int. J. Risk Assessment and Management*, Vol. 26, No. 2, pp.175–195.

3.3 Introduction

Climate, social, geopolitical, and technological changes create an extremely complex and volatile environment to which organisations must continually adapt (Jacob and Michel, 2020). These changes contribute to the advent of 'new' risks, described as emerging, whose characteristics make them very difficult to manage by traditional RM processes (International Risk Governance Council

[IRGC], 2018). To address these risks, more global approaches, qualified as 'integrated' and based on the concept of risk governance, are required. In that sense, depending on their field of activities or their objectives, the literature offers organisations multiple reference frameworks, such as the Control Objectives for Information and Related Technologies (COBIT) framework for information technology management and governance (Information Systems Audit and Control Association [ISACA], 2012), the Committee of Sponsoring Organizations (COSO) Enterprise Risk Management Framework (COSO, 2004), the IRGC risk governance framework (IRGC, 2017), the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2018a), among others. A plethora of IT tools (so-called enterprise RM tools) are also available to organisations[7].

Despite the range of frameworks and tools available to organisations, many that try to implement integrated risk management (IRM) initiatives have great difficulty in doing so (Jean-Jules and Vicente, 2020). Indeed, many organisations turn to IT tools to implement IRM, thinking the tools will do all of the work. However, such tools have little tolerance for uncertain or ambiguous applications and omit any consideration of human and social dimensions of risks (Jean-Jules and Vicente, 2020). However, the real challenge of IRM lies specifically in its social and organisational aspects. In addition, organisations do not seem to question their method of approaching and managing risks, which is in fact the problem that IRM is designed to resolve (Amansou and Chaouki, 2019). IRM is first and foremost a question of risk governance (IRGC, 2018). It must be approached as such and not solely as a project aimed at implementing IT tools (Amansou and Chaouki, 2019). Thus, it is clear that the progress made in the field of RM, which can be assessed by the extent of the scientific literature available, does not easily translate into significant gains at the level of organizations, even though, ultimately, it is largely up to them to manage risk.

Therefore, there seems to be a certain disconnect between what the scientific literature advocates and what is done in practice by organizations. This can be explained, among other things, by the fact that in organizations, practitioners responsible for managing risks might lack the required competency in this area or sufficiently detailed knowledge of the science of risks than do researchers in this field (Jean-Jules and Vicente, 2020). They are therefore not necessarily able to fully grasp its complexity in the finest detail. In addition, when analyzing the existing literature on

[7] From Capterra.com: https://www.capterra.com/integrated-risk-management-software/.

IRM and emerging risks, one can imagine the difficulty that may be encountered by practitioners searching for documents that explain the difference between emerging risks and traditional risks, and how the former should be managed.

Thus, the first section of this paper will present the concept of traditional risk and its management. This will allow the reader to better understand and appreciate the second part of the paper, which will present the concept of emerging risks and the particular challenges related to their management. Finally, the third part of the paper will present the concept of IRM and show why emerging risks should be addressed as a risk governance and social constructivism challenge. Based on this, the paper concludes by highlighting the importance for organizations to define and implement a collaborative structure dedicated to IRM and the importance of taking into account individual risk perceptions when implementing IRM frameworks.

3.4 Risk and RM: The traditional context

3.4.1 Traditional risk: A concept based on the exact sciences

Risk is a mathematical concept that was first introduced by Christiaan Huygens. It is defined as the mathematical expectation of a random variable (Huygens, 1714). In concrete terms, the mathematical expectation (E) of a discrete random variable $\bar{C}$ corresponds to the weighted average value that one can expect to obtain if one repeats experiment $\bar{C}$ many times. Thus, the mathematical expectation of an event $\bar{C} = (c_1, c_2, \dots, c_n)$ with the associated probability vector $\bar{P} = (p_1, p_2, \dots, p_n)$ is:

$$E(\bar{C}) = \frac{\sum_{i=1}^{n} p_i c_i}{\sum_{i=1}^{n} p_i} \tag{1}$$

Assuming that all events c_i of the random variable $\bar{C}$ are known and that the probability p_i of each is also known, then $\sum_{i=1}^{n} p_i = 1$ and the formula becomes:

$$E(\bar{C}) = \sum_{i=1}^{n} p_i c_i \tag{2}$$

For example, the mathematical expectation associated with throwing a balanced cubic die is:

$$E(\bar{C}) = \sum_{i=1}^{n} p_i c_i = \frac{1}{6} \times 1 + \frac{1}{6} \times 2 + \frac{1}{6} \times 3 + \frac{1}{6} \times 4 + \frac{1}{6} \times 5 + \frac{1}{6} \times 6 = 3.5 \quad (3)$$

Mathematical expectation is based on two parameters: probability and consequences. In RM, the mathematical expectation formula becomes the risk (R) formula, which is traditionally expressed as the product of the probability that a hazard will occur (P) and its consequences (C) (International Organization for Standardization (ISO), 2002):

$$R = P \times C \quad (4)$$

This definition of risk, which is called 'traditional', comes from mathematics. Thus, it is based on the exact sciences. It is also focused on hazards and addresses only one event at a time, namely the effects of one hazard on one system. To quantitatively assess risk, one must therefore (1) know the hazard, (2) be able to assign it a probability of occurrence, and (3) be able to measure or quantify the consequences of this hazard for the system in question. Now, unlike games of chance, where the probability of an event can be determined according to a finite number of contingencies and where the consequence is known, it can be very complicated to assign values to risk parameters in the real world. Thus, in practice, a more subjective approach (semi-quantitative or qualitative) can be used to give risks an order of magnitude (low, medium, high) (IRGC, 2018). In that case, instead of using the term *probability*, which refers to the exact mathematical concept, we will use the word *likelihood*. As the ISO (2018, 4) puts it, '…"probability" is often narrowly interpreted as a mathematical term…. in risk management terminology, "likelihood" is used to refer to the chance of something happening, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms'.

3.4.2 RM: A process adapted to the traditional risk context

RM in a traditional risk context (also called 'traditional RM') is a process intended to identify, analyze, and evaluate risks (one by one, threat by threat) to determine which ones are acceptable to the organization, and which ones are not and must therefore be treated (ISO, 2018). Figure 3.1 illustrates this process.

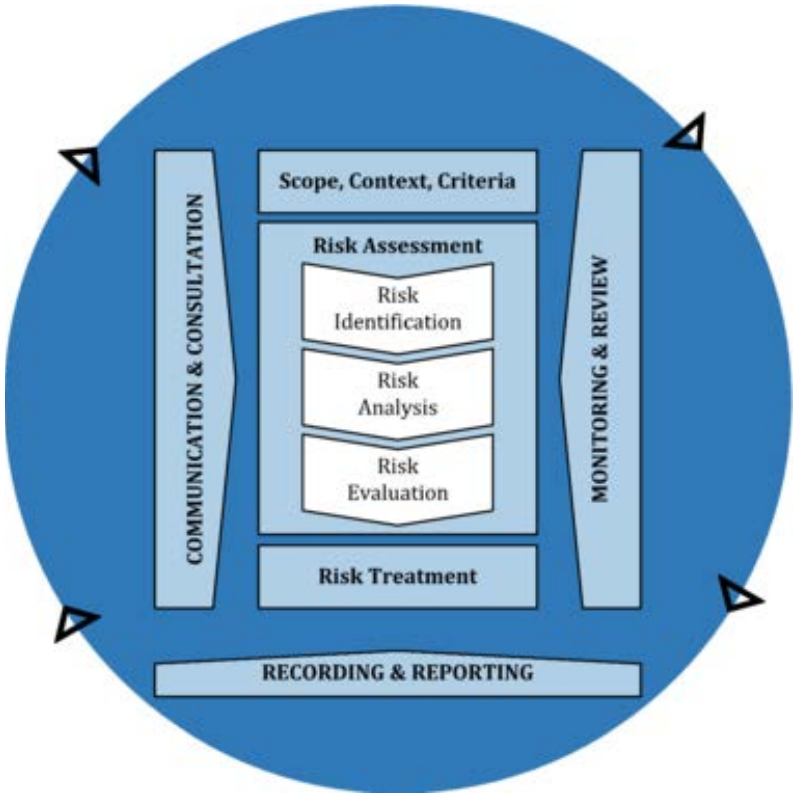


Figure 3.1 ISO RM process (ISO, 2018)

The first phase of RM establishes the context and objectives of the study; this phase allows users to determine the scope of the study and identify analysis techniques, methods and the criteria that will be used in the subsequent phases of the process, namely risk assessment and risk treatment. Risk assessment is the core of the RM process. In its first two steps – risk identification and risk analysis – hazards (often associated with dangers) present in the environment (internal or external) of the system are identified and a risk value is assigned to them based on their probability of occurrence (likelihood) and their anticipated consequences for the system being studied. In the third step – risk evaluation – risks are classified, ranked and compared to a threshold value (acceptability threshold, tolerance threshold) set by the organization as a function of its risk aversion (or risk appetite). Typically, at this step, a risk heat map is used to do the comparison. A risk heat map is a matrix divided into zones (e.g., green, yellow, orange, red), each of which is associated with a range of risk values (e.g., green: 0% to 25% (negligible risk); yellow: 25% to 50% (low risk); orange: 50% to 75% (moderate risk); red: 75% to 100% (high risk)). Figure 3.2 shows a typical risk heat map.

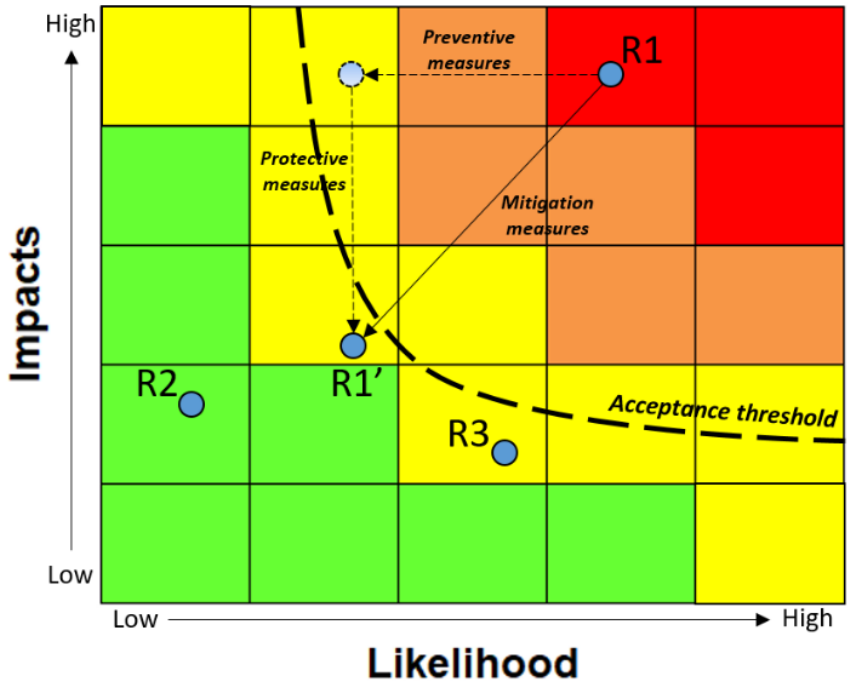


Figure 3.2 Typical risk heat map

In this heat map, we can see four risk zones and the acceptability threshold defined by a fictional organization. Three risks (R1, R2 and R3) are also shown. Of these risks, only R1, whose value is located above the threshold value, should be subject to treatment to reduce it to an acceptable level (illustrated by point R1'). This treatment corresponds to the third phase of the process and consists of identifying and implementing mitigation measures (preventive or protective) designed to reduce risks. At the end of this third phase, the analyzed risks should theoretically all be located below the organization's acceptability threshold. Finally, the process provides for risks to be the subject of communication and consultation, follow-up and recording to ensure that they are disseminated, known about, periodically reviewed and documented (ISO, 2018).

3.5 Emerging risk: Change of context, change of paradigm

3.5.1 Emerging risk: A concept based on uncertainty

For some time now, climate, social, economic, geopolitical and technological factors have resulted in profound changes in the environment; these are reflected in a transition from traditional risks to 'new' risks, which are known as emerging risks (United Nations Office for Disaster Risk Reduction

[UNDRR], 2019). According to the Institute of Risk Management, an emerging risk is ‘a risk that is evolving in areas and ways where the body of available knowledge is weak’ (Salim et al., 2021, 6). For the International Risk Governance Council (IRGC, 2018, 1), emerging risks are ‘new risks or known risks that develop in new context conditions and are unfamiliar to their managers’.

Overall, several categories of emerging risks can be distinguished. It should be noted that there is some overlap between categories such that a given event could have the characteristics of one or more of them and, in particular, could transform and evolve from one category to another:

- **Catastrophic risks** are related to extremely rare and relatively sudden events that normally affect delimited regions that are not traditionally known to experience this kind of event (Perfors and Van Dam, 2018). These risks are often associated with Black Swan Theory (Taleb, 2010). The Quebec Ice Storm of 1998 (Gouvernement du Québec, 1999) and the Fukushima nuclear accident of 2011 (International Atomic Energy Agency [IAEA], 2015; Tokyo Electric Power Company [TEPCO], 2012) are two examples of catastrophic risks.
- **Systemic risks** are related to interdependencies and interconnections among systems. This means that a failure in one system can propagate to other systems by means of a domino effect (UNDRR, 2019). The blackout in the northeastern United States and Canada in 2003 (Natural Resources Canada [NRC] and United States Department of Energy [US DOE], 2004) is an example.
- **Femtorisks** are due to minor disruptions or events (whence the prefix *femto* $=10^{-15}$), which would usually remain unnoticed but, in specific contexts or conditions, can give rise to cascading chaotic phenomena (Frank et al., 2014). These risks are often associated with Chaos Theory (and its butterfly effects) and characterize many complex adaptive systems that are sensitive to the initial conditions (Su, 2021). The disruption of the global supply chain (which was already substantially weakened by the closure of many factories as a result of the public health measures imposed due to COVID-19) in 2021, followed by the blockage of the Suez Canal by a container ship, is an example of a femtorisk (Lee and Wong, 2021).
- **Hyper-risks** originate from the interdependencies among different areas of activity (social, economic, political, technological, among others), which give these risks the capacity to affect several aspects of society at once (Ray-Bennett et al., 2014; UNDRR, 2015). Financial crises are examples of hyper-risks.

- **Cyber-risks** are due to deliberate actions committed by individuals or states with the intent of penetrating individuals' or organizations' information systems to paralyze their operations, take control of the systems, or steal, erase or compromise information to cause harm or obtain a benefit (ISO, 2009; National Institute of Standards and Technology [NIST], 2008). Phishing, denial of service attacks, and ransomware are examples of cyber-risks.
- **Hybrid risks** (or hybrid threats) are due to deliberate actions committed by individuals or states to harm, destabilize, or influence powers (organizations in power) or public opinion, hampering decision-making processes or creating disinformation to create friction (tension, disorder) in the social fabric (European Commission, 2016). Foreign interference in elections in democratic nations to influence the results is an example of a hybrid risk.
- **Existential risks** are risks whose impacts could endanger the survival of an organization, a population or, in the most extreme case, all of humanity. For example, changes in consumer habits and technological change (innovation) may lead to the disappearance of an organization or a whole industry; demographic changes linked to population growth and climate change could lead to the disappearance of a community, a culture, or all of humanity (UNDRR, 2019). The COVID-19 pandemic is an example of an existential risk.

Although the concepts of newness and emergence are relative, emerging risks are characterized by a higher level of uncertainty than traditional risks because one or more of the risk parameters is new, ambiguous, or uncertain for the people who have to deal with these risks (IRGC, 2018; Salim et al., 2021). According to Hopkin (2018), this uncertainty is related to a lack of knowledge, which may concern the event underlying the risk or the context in which it materializes. Depending on the source of this lack of knowledge, an emerging risk may be classified in one of the following three categories: (1) a known event in a new context, (2) a new event in a known context, or (3) a new event in a new context (Hopkin, 2018). The context here is related to all of the conditions (social, economic, political, climatic, structural, among others) characterizing the system being studied and its environment when the risk materializes. It is therefore dynamic and changing.

In addition to being more uncertain, emerging risks are more complex than traditional risks (IRGC, 2018). This complexity is due to interdependencies among systems, networks, and different areas of activity, but also between the risks themselves. For example, a hurricane could create a flood which in turn could create a landslide which in turn could impact a power plant, generating a major

power outage over a vast territory. The multidimensional nature of emerging risks and their interdependencies, coupled with the interdependencies among systems, create a very complex ecosystem in which emerging risks are no longer necessarily the outcome of linear causal reactions related to a specific hazard and its direct consequences for the system, but rather of sudden or latent conditions – exogenous, endogenous or inherent in systems. The result is that a given disruption may degenerate into one or more series of cascading (escalating) events that exploit the vulnerabilities of systems and interconnections among systems to propagate from one to another by means of a domino effect (IRGC, 2018; Robert and Morabito, 2008). As a result, emerging risks cannot be addressed using traditional approaches that focus on one risk at a time because these approaches were not meant to deal with interdependencies between hazards or the cumulative/conditional impacts of multiple hazards (multi-hazards) (Gilbert et al., 2016). Rather, they must be addressed using all-risk approaches since they must be studied in all their facets at the same time. This requires analyzing them through multiple lenses, whether from a technical, environmental, social, financial, or political perspective, among others.

The characteristics of emerging risks raise several questions regarding our real capacity to evaluate these risks according to the traditional definition of the concept of risk. Although this definition is still widely disseminated and used, experts have been exposing the limitations of this definition and casting doubt on it for several years (Purdy, 2010). For example, in 2004, Australia and New Zealand changed the definition of risk in *AS/NZS 4360:2004* to the following: 'the chance of something happening that will have an impact on objectives' (Standards Australia, 2006, 3). And, since 2009, the ISO has also proposed a new definition of the concept of risk, defining it as 'the effect of uncertainty on objectives' (ISO, 2009, 3).

This 'new' definition of risk presents two particularly interesting elements and marks an important change of paradigm regarding how risks are (or should be) managed. First, this definition now associates risk with uncertainty, which is paradoxical to say the least, since risk and uncertainty are essentially two different – even, to some extent, opposite – concepts. Uncertainty, which was introduced by Frank H. Knight, translates as a lack of information or knowledge about both the hazard and its consequences, meaning that the situation is one that cannot be evaluated in terms of risk (Knight, 1921). Thus, by aligning the concepts of risk and uncertainty, the new definition recognises *de facto* that, in some cases, there is insufficient knowledge to really assess the risk – that is, identify, analyse and evaluate it – and that instead, the situation is an uncertain one in which

risk cannot be determined. Second, whereas the traditional definition of risk centred on hazard, this new definition focuses more on consequences. The expression ‘effect of uncertainty’ points directly to the consequences of uncertainty and not to its causes. Thus, the new definition guides RM toward the management of risks’ consequences. By specifying that the effects concern objectives, the new definition orients analysis toward the study of the system and its mission. The scope of this new definition is therefore much more strategic and better aligned with the challenges presented by the management of emerging risks.

3.5.2 Challenges related to emerging RM

The characteristics of emerging risks give rise to several challenges affecting their management. These challenges are mainly caused by the difficulty of assessing – that is, identifying, analysing and evaluating – these risks relatively objectively.

First of all, one of the main challenges related to emerging RM relates to the difficulty of quantifying these risks. Traditional RM is based on the premise that hazards are known and that information and knowledge allowing managers to assess their probability of occurrence (likelihood) and their potential consequences are also known, or at least exist. This fundamental condition does not apply in the case of emerging risks. Instead, the characteristics of emerging risks ensure that organizations face more uncertainty, that is to say, situations in which knowledge is inadequate to assess the possible eventualities or consequences associated with them with any degree of confidence (IRGC, 2018; UNDRR, 2019). In some cases, no information exists that would allow people to identify or analyse a risk; in other, more extreme, cases, knowledge is inadequate to even imagine the existence of a risk (here, we are speaking of radical uncertainty, also known as Keynesian uncertainty or ignorance, referring to the work of John Maynard Keynes) (Keynes, 1936; Runde, 1990; Stohs, 1980). The traditional approach to RM is unable to manage unknowns (Gilbert et al., 2016). Furthermore, in focusing on the probability of occurrence (likelihood), the traditional approach intuitively takes it for granted that history repeats itself and past events are, in some sense, indicators of the future, which is not necessarily true in a constantly changing world; thus, this approach cannot bring emerging risks to light (Gilbert et al., 2016; Organization for Economic Co-operation and Development [OECD], 2003).

The difficulty associated with the identification and quantification of emerging risks is aggravated by the fact that the relationship between hazards and their consequences is a nonlinear one.

Traditional RM intuitively assumes that the causal link between a hazard and its impacts has a certain linearity (indeed, it is direct) (OECD, 2003) and is circumscribed in time and space, as shown by the use of risk heat maps like the one in figure 3.2. This hypothesis is not confirmed for emerging risks, since they are able to cross all borders (geographic, social, technical or organizational). They can also be extremely volatile, in that they may change very slowly or very fast and propagate chaotically between different systems, very locally or over huge territories, and with a very short or very long time horizon (UNDRR, 2019). Thus, emerging risks are extremely difficult to circumscribe in time and space since their consequences are not necessarily the result of a single hazard, but rather the result of a conjunction of a set of conditions. It is therefore impossible to establish a direct link between a hazard and its consequences, since a multitude of causally related intermediate phenomena may come between them. In addition, even though it may be relatively easy to trace back the cause of a failure once the incident has happened (*a posteriori* or post-accident analysis), it is much more difficult to do so preventively (*a priori* analysis) since an infinite number of scenarios is possible at that point (UNDRR, 2019). It therefore becomes very difficult to assess a risk based on the probability of occurrence (likelihood) of the hazard and its consequences because the probability, in these conditions, tends to zero.

Another challenge of emerging risks concerns their evaluation. Traditional RM tends to represent risks within a static model (typically, a risk heat map). Although such a representation may be correct in the context of traditional (or operational) risk, it reaches its limits when it comes to representing emerging risks. As discussed above, emerging risks are difficult to identify and quantify. It is therefore very difficult to position them on a heat map. Even if that were possible, emerging risks are very dynamic. They vary as a function of changes in the environment. These changes modify the context in which such risks materialize, meaning that a given event could have only minor consequences in one particular context but completely different, even major, consequences in a different context. Thus, emerging risks are difficult to represent with static points on a map given that they are constantly ‘moving’. Moreover, even the risk acceptability threshold, a static benchmark, does not take context into consideration. This circumstance may mean that a risk that is acceptable today (in a given context) is unacceptable tomorrow (in a different context), and vice versa. As a result, the risk acceptability threshold is not only dynamic, it also varies depending on the risk. Given two different risks, an organization may have a very high tolerance threshold for one and a very low one for the second. Thus, there is not one single acceptability

threshold, but several, so the threshold cannot be given a static or unique value. It is therefore extremely difficult, if not impossible, for an organization to establish a threshold in any coherent way.

As an added complication, the theory that an organization can determine this threshold on its own is invalid in a context of emerging risks, where consequences extend far beyond the borders and responsibilities of a single organization. Today, the acceptability of a risk cannot be decided on by one organization (or a few managers), but rather must be subject to discussion and consensus involving all stakeholders, including the populations that will suffer the consequences, based on their perception of what this risk represents for them (IRGC, 2020). What is acceptable to one person (or group of people) may not be acceptable to others. This question of risk perception or behaviour in the face of risk (attributable to the human factor) is crucially important and must be taken into account. The human factor cannot be reduced to a mathematical equation, since it depends on numerous factors other than probability and consequence (Kmiec and Roland-Lévy, 2014); most of these factors are subjective but nonetheless legitimate (OECD, 2003). This issue must be analyzed in depth, taking into account not only experiences, fears and other social factors but also all of the advantages and disadvantages that the risk represents for the parties exposed to it (Barnett and Breakwell, 2001; Sjöberg, 2000). This is especially true for emerging risks, where uncertainty is very high. Now, although this factor might be relatively predictable in a context of known risks (e.g., the context of operational risks), it is much more complicated to weigh the effects of the human factor as a source of increased or decreased risk or the effects of the acceptability of a highly uncertain risk (Beghetto, 2021; OECD, 2003). The human factor becomes predominant in a context of uncertainty, but traditional RM does not directly incorporate parameters related to this factor (perception, behaviour) into analyses (OECD, 2003).

The key role of the uncertainty surrounding emerging risks and their propensity to propagate from one system to another makes them very hard to control with traditional processes, first because they are difficult to measure, and second because their management does not depend on a single organization responsible for them but rather on all affected organizations (Salim et al., 2021), including the populations that may ultimately suffer the consequences (IRGC, 2020). Thus, these risks cannot be isolated from each other such that they can be analysed one at a time, and their management cannot be entrusted to a single organization (OECD, 2003). In this context, as complexity, uncertainty and ambiguity rise, more stakeholders need to be engaged in the RM

process, from civil society, who in the end suffer the consequences of risks, to regulatory authorities who will have to assume a greater role by putting in place policies that foster multi-organizational collaborations, to organizations themselves, which will have to take into account the effects of their failure on other organizations and on the population and put in place more coordinated and transparent response mechanisms (IRGC, 2020). All of this goes far beyond the framework of the traditional RM approach, which, although it is well adapted to operational risks that arise in relatively well-known environments/contexts (controlled to some extent and circumscribed in time and space), it is unable to deal with problems that are more complex. Thus, when faced with the challenges of emerging risks, the traditional RM approach of focusing on the analysis of one threat at a time (hazard-by-hazard analysis) reaches its operating limits. It was never designed for that purpose and is therefore of very little use in effectively addressing emerging risks (IRGC, 2018; UNDRR, 2019). In light of this observation, organizations are encouraged to make a sustainable transition toward IRM, an approach that is better aligned with the challenges presented by emerging risks (UNDRR, 2015).

3.6 IRM: A more strategic, cross-cutting approach to managing risks

3.6.1 What is IRM?

The concept of IRM first appeared in the financial sector in a context in which the traditional RM approach was being questioned. Following the various corporate scandals and bankruptcies of the 1990s, in 2002 the United States adopted the *Sarbanes-Oxley Act* to introduce new corporate governance rules, particularly with respect to financial RM and internal control, which were required to become more integrated (Arena et al., 2010; Dionne, 2013). Over time, the scope of the concept gradually expanded to other areas of RM.

IRM was born of the inadequacy or inability of traditional RM to handle cross-cutting problems: As explained previously, because it considers risks in isolation, hazard-by-hazard, traditional RM possesses major limitations (Amansou, 2019; Amansou and Chaouki, 2019; UNDRR, 2019). IRM contributes a new organizational dimension. While traditional RM refers to a process of systematically evaluating risks that apply locally or operationally, IRM involves the implementation of a global RM strategy throughout the organization (Oliveira et al., 2019).

According to the Government of Canada (2016), IRM must be decompartmentalized and must promote a systematic, continuous, proactive approach that aims to understand, manage and communicate risks from the perspective of the entire organization in a coherent, structured way. In the view of Bohnert et al. (2019), IRM is a consolidated approach throughout the organization representing a paradigm shift, consisting in the movement from a siloed RM approach to a more cross-cutting, corporate-wide approach that allows for a holistic, strategic vision of risk. To achieve this, IRM must undeniably consider the work that is done at the local and operational levels (traditional RM), but above all, it must be aligned with the organization's overall mission (Amansou, 2019; Oliveira et al., 2019). To this end, IRM must create value for the organization and allow for decision-making that contributes to the achievement of its strategic objectives (Bohnert et al., 2019).

IRM enhances general risk theory (i.e., traditional RM) with joint action theory (Amansou and Chaouki, 2019). Joint action theory designates the intention behind the action and is constructed based on strategies and principles that orient actions toward the achievement of a common vision (Simard, 2007). In this context, unlike traditional RM, which is seen as a process, IRM appears to be more of a question of governance, with regards to the manner in which RM should be orchestrated within an organization, calling directly upon the notions of risk governance (IRGC, 2005).

3.6.2 Governance: The key element of IRM

The word *governance* comes from the Greek *kubernân* and the Latin *gubernare*, which means to steer a ship (Caron et al., 2020). The word was first applied to politics around 400 BC when Plato used it to express the action of leading a group of people – or the 'art of governing' (Brouillette, 2009). There is a clear etymological link between the words *governance* and *government*.

Lacroix and St-Arnaud (2012) conducted an interesting review of the concept of governance. Citing several sources, they explain that the social, economic, and political upheavals of the 1970s to the 1990s highlighted the difficulty that governments had in responding to growing social needs; consequently, the concept of governance regained its currency with a new meaning. This 'new' governance was intended to promote a new type of administration based not on the centralization of powers but on sharing (redistribution) and decentralization of powers, a redefinition of roles and responsibilities, and a transformation of relationships between governments and their citizens, the

aim of which was to ensure greater transparency and increased citizen participation. The scope of the concept of governance was gradually expanded and applied more generally to management sciences. In this domain, Merriam-Webster defines governance as 'the act or process of governing or overseeing the control and direction of something (such as a country or an organization)'.[8]

Governance should pave the way for negotiation, cooperation, and partnership among different actors, each of which holds a certain form of power and shares its responsibilities to achieve common goals established collectively. Governance should allow for harmony, coherence, and convergence, offering a more precise framework for stakeholders and their actions (Lacroix and St-Arnaud, 2012). In this sense, governance is a form of multi-stakeholder steering, the implementation of which depends on a set of tools including rules, standards, and protocols, among others, designed to ensure better coordination of stakeholders, each of whom has a share of power, to make decisions in consensus and launch joint actions (Fernandez, 2018). In this context, decisions are no longer made by a single decision-maker (or group of decision-makers), but rather the outcome of co-development by all the actors and stakeholders involved in the common cause (Fernandez, 2018). This phenomenon is part of a transformation of the management approach from a vertical hierarchy to a more horizontal structure, centered on stakeholders and focusing on collaboration and participation (Lacroix and St-Arnaud, 2012). Governance is particularly important in a context in which several stakeholders (or organizations) are active and there are no hierarchical relations among them. This is the case with collaborations among several functional units within a single organization or several different organizations involved in a common cause.

According to the Institute for Governance of Private and Public Organizations (IGOPP) (2022), governance must be part of a value-creating approach. For Fernandez (2018), value creation must be reflected within each stakeholder through discussions among them. Value creation has also been highlighted as one of the fundamental conditions that allow multi-organizational collaboration to be maintained over the long term (Morabito and Robert, 2023a). For a collaborative arrangement to be sustainable, it must give the participating organizations value that they could not otherwise acquire. This value is directly related to shared knowledge, enabling new collective knowledge to be created (Kodama, 2005a).

[8] From Merriam-Webster online: https://www.merriam-webster.com/dictionary/governance.

According to IRGC, risk governance consists of applying the principles of good governance to RM. This calls for RM to be a more distributed, cross-disciplinary, and collaborative (IRGC, 2018). In this way, RM is no longer the business of a single unit that is responsible for it, but rather of the whole organization, bringing all organizational stakeholders into play and, therefore, becoming 'integrated'. This must be part of a structured, coherent, concerted approach by the whole organization. To this end, IRM must be conceptualized, organised, and directed by a competent entity within the organization that has a specific mandate to do so (Morabito and Robert, 2023a), however its actions must be decentralized to all organizational actors, what IRGC calls 'distributed governance' (IRGC, 2018, 55). This requires the implementation of a specific risk governance framework that enables it to achieve the desired strategic, cross-cutting dimension. Figure 3.3 illustrates the elements that a governance framework for IRM should include.

Figure 3.3 Key elements of governance

IRM must be aligned with the organization's mission, vision, and objectives, which define the common cause in which actors are engaged. Through policies, directives, guidelines, norms, and standards, IRM must guide and formalize RM by providing a holistic vision of how this management should be applied and integrated within the organization. By clarifying the processes to be followed by each actor/stakeholder and their roles and responsibilities, IRM should position these actors at the core of RM at all organizational levels, thereby promoting the decentralisation

of RM. By giving these actors a common framework (or reference system) for their actions and providing clear indicators for decision-making, IRM should ensure the coherence (synergy) of all of these actions for achieving the organization's strategic goals and mission. In that way, it comes full circle and connects with joint action theory (discussed above) by promoting notions of social construction.

3.6.3 Social constructivism: From multidisciplinarity to transdisciplinarity, reducing risks by increasing collective knowledge

From a perspective in which risk is associated with uncertainty, reducing risk amounts to reducing uncertainty. Uncertainty being the result of a lack of knowledge (Hopkin, 2018), we can therefore hypothesize that, the more we increase knowledge, the more we reduce uncertainty and, *ipso facto*, risk. For an organization (or group of organizations), reducing risks therefore amounts to increasing knowledge of those risks. This knowledge is collective: it is not held by a single person and must therefore be constructed based on discussions amongst the stakeholders involved. In this sense, IRM calls upon notions of social construction and highlights concepts from social constructivism.

Social constructivism is a theory developed by Lev S. Vygotsky that describes learning as an active process of co-construction during which knowledge is constructed further to social interaction (Vygotsky, 1978). By connecting existing knowledge, we allow new knowledge to be created (Adams, 2006; Tašner and Gaber, 2020). One of the characteristics of emerging risks is that they are able to cross knowledge boundaries (disciplinary or new knowledge), which means that not only is multidisciplinary knowledge required to identify them, but transdisciplinary knowledge is required to understand them. Transdisciplinarity is necessary to understand complex sets of problems (Gooding et al., 2022) and is the only way forward to reduce complexity in risk assessment. To achieve this, IRM must incorporate a cyclical, incremental value creation process, whereby shared individual knowledge (both tacit and explicit) makes it possible to build collective knowledge, which itself rebuilds individual knowledge and allows for the construction of new collective knowledge; the process continues iteratively until a cross-cutting understanding of the problem in question is developed (Kuraoka et al., 2020). This can only be constructed through long-term collaboration, since the fruits of collaboration can only be gained over the long term (Morabito and Robert, 2023a). Thus, IRM must give the stakeholders a preferential locus for discussion (a space or forum) that is adapted to this context. Robert et al. (2007) define this space

as a ‘cooperative space’. The cooperative space requires a long-lasting collaboration structure to be put in place to allow the aggregation of knowledge within a common reference system. It also requires a competent facilitator to guide the stakeholders toward analyses that will ultimately allow their understanding of the problem in question to be expanded (Morabito and Robert, 2023a).

In the case of IRM, what should the expanded understanding include? In other words, what knowledge should the organization develop and/or enhance? Since risk is defined as ‘the effect of uncertainty on objectives’, understanding must cover two aspects: (1) the organization’s objectives, and (2) the sources of uncertainty. Regarding the first aspect, the organization must increase the knowledge it has of itself. That involves knowledge of its basic mission, which is reflected in the provision of a resource (or service) in the environment (Robert et al., 2007). It is broken down into strategic objectives, which are divided into several activities distributed throughout the organization and assigned to different functional units. The execution of these activities requires different elements (infrastructures, processes, systems, actors, resources, among others), each of which contributes, to some extent, to achieve the organization’s mission. In this context, the increase in knowledge must focus on understanding how these various elements function, how they are interconnected and interact, what their vulnerabilities are, and to what extent damage affecting one of these elements may impact the organization’s mission (e.g. what are the impacts of their failure).

The second aspect, the identification of sources of uncertainty, is particularly difficult since uncertainty is quite an abstract, even subjective, concept. The challenge for the organization is therefore to identify the sources of uncertainty and increase its knowledge of them so it can gradually dissipate this uncertainty. To do this, the organization must pay attention to its internal and external environments. These environments are characterized by a multitude of dynamic parameters (environmental parameters) of different kinds (technical, economic, political, climatic, social, and legal, among others). The scope of knowledge of these environments is practically infinite, so it is impossible to characterize them precisely. On the other hand, by using a consequence-based approach (Robert et al., 2007), it is possible to perceive the environmental parameters that are most likely to affect each of the elements that contribute to the organization’s mission and, consequently, the mission itself. The challenge for the organization is, therefore, to acquire information on these environmental parameters and interpret, analyze and correlate them correctly, so that they may be translated into indicators representing the state of the environments

(i.e., the context). These indicators must be capable of projecting a situation in which a negative event is anticipated or a situation in which an opportunity is possible. These three actions (perception, representation, and projection) will allow the organization to develop its situational awareness (Endsley, 1988, 1995). The organization's ability to orient its decisions (act/react) as a function of the information conveyed by these indicators reflects its resilience, or ability to adapt to real or anticipated changes (disruptions) in its environment and continue to function despite them (Micouleau and Robert, 2021; Micouleau et al., 2020).

In this context, the conclusion we can draw from the available literature is that IRM is no longer solely an operational process whereby the organization protects itself from potential hazards, but rather becomes a highly strategic activity entailing the acquisition and growth of collective knowledge that constitutes an integral part of the organization's decision-making process. Risk assessment is no longer a process intended to calculate risk values for particular hazards, but rather an activity whereby the organization develops its situational awareness by analyzing and correlating relevant environmental parameters and translating them into indicators to anticipate events that could impact its objectives and proactively take action to steer the organization through changes in its environment toward the achievement of its mission and increase its resilience. Organizations who are seeking to implement an IRM governance framework must clearly understand these differences.

3.7 Discussion and conclusion

Organizations operate in increasingly uncertain contexts. Climate, social, geopolitical, and technological changes completely transform the environment, making it extremely volatile. As these environmental changes occur, the levels of complexity, ambiguity and uncertainty surrounding risks increase, exacerbating the transition from traditional risks to emerging risks. Thus, there exists a tipping point (more of a zone) where traditional RM approaches no longer provide sufficiently accurate results. Beyond that zone, organizations must change how they manage risks, moving from a more traditional approach based on analyses of failure scenarios, mathematical approaches and infrastructure protection, to an approach that is based more on governance and socio-constructivism, that is the expansion of collective knowledge (i.e., understanding the organization's assets, operations and environment) and the building of the

organization's resilience and adaptability to its changing environment. This so-called 'integrated' RM approach is much more cross-cutting and requires more communication, collaboration and coordination amongst all stakeholders in the organization and in society more generally, which calls for implementing solid governance. Figure 3.4 summarizes this.

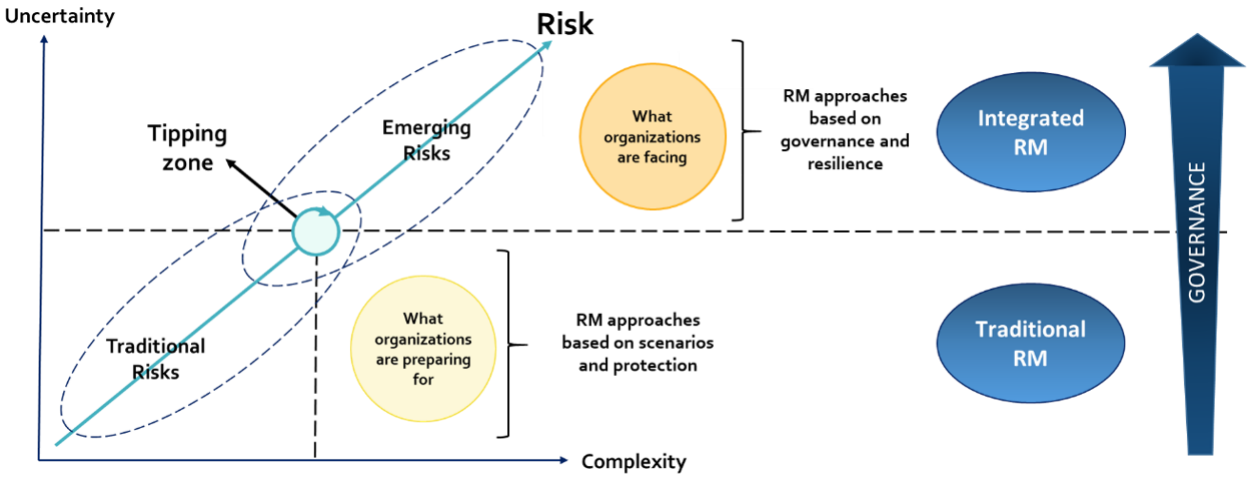


Figure 3.4 Illustration of the transition from traditional RM to IRM

Although multiple frameworks and tools exist, the reality is that RM in organizations is still largely done in silos and organizations must find a way to break down those silos for these frameworks and tools to be efficient and bring added value. In that sense, IRM demands a real commitment by the organization and a profound change in organizational culture going from a more vertical RM structure to a transversal RM structure. Change triggers resistance, *a priori*; more importantly, it requires planning, management, and support. To achieve this, IRM cannot be improvised within an organization. It must be organized by people who have the necessary competencies and knowledge of RM to develop and implement such an initiative. However, its operationalization must be decentralized to all the organizational actors. This of course requires a specific risk governance framework to be adopted by the organization, but it mainly requires a long-term collaboration structure (or cooperative space) to be put in place to allow the organizational actors to exchange knowledge on risks and aggregate them within a common reference system. This will allow the organization to have a better understanding of its environment and systems and obtain the relevant indicators it needs to guide its decisions.

A first challenge for the organization is therefore to determine the shape that a cooperative space must have and how it should be integrated within the organizational structure. The objective in that

sense is not to drastically change the functional organizational structure, which is efficient for dealing with daily operations, but rather to make it possible for transversal initiatives to coexist harmoniously within the structure. A second challenge results from the decentralization of RM: By positioning actors at the heart of RM, perception bias (subjectivity) is introduced into risk assessments. This bias must be reduced to a minimum. As more work will need to be done to address these challenges, one fact remains: While most organizations see risk as an outside ‘enemy’, the greatest risk an organization faces is inherent in the way it manages them.

CHAPITRE 4 MÉTHODOLOGIE DE RECHERCHE

La rétrospective du projet DOMINO a permis d'identifier un sujet de recherche en la GIR chez les grandes organisations. La revue des défis liés à la gestion des risques émergents suggère que la GIR est avant tout une question de gouvernance relative à la manière dont l'organisation gère les risques par le biais de toutes les parties prenantes impliquées. Ces deux articles conduisent donc à la problématique qui est au coeur de cette recherche doctorale : la gouvernance relative à la GIR chez les grandes organisations.

Ce chapitre vise à présenter la méthodologie de recherche qui sera employée afin d'adresser cette problématique. Ainsi, la section 4.1 présente les hypothèses à la base de ces travaux de recherche et la question de recherche qui découle de ces hypothèses. À la section 4.2, la question de recherche est scindée en objectifs général et spécifiques à atteindre. Finalement, la section 4.3 présente le contexte dans lequel seront réalisés ces travaux ainsi que la méthodologie de recherche, adaptée à ce contexte, qui sera employée pour atteindre les objectifs poursuivis et, en définitive, répondre à la question de recherche.

4.1 Hypothèses et question de recherche

Les travaux sur DOMINO ont permis d'établir le constat à l'effet que les réponses aux problématiques nouvelles et complexes, comme les risques émergents, ne s'obtiennent qu'en mettant en commun des informations et des connaissances multidisciplinaires provenant de plusieurs sources. Ainsi, lorsqu'adéquatement agrégées et corrélées, ces informations et connaissances multidisciplinaires arrivent à générer des connaissances collectives nouvelles, davantage transdisciplinaires celles-ci, qui aident à la compréhension des risques et qui permettent de prendre des décisions plus éclairées visant à les réduire, voire les éliminer à la source, lorsque cela est possible.

Ce constat semble d'ailleurs renforcé par le fait qu'après un accident, une analyse (ou enquête) permet, dans la plupart des cas, de reconstruire la genèse de cet accident pour en arriver à la conclusion que les informations qui auraient permis de le prévenir existaient déjà à la base, avant même que l'accident ne se produise (UNDRR, 2019). Cependant, comme ces informations

n'étaient pas disponibles à l'intérieur d'un référentiel commun, elles n'ont pu être agrégées/corrélées et interprétées/rapportées correctement – ce qu'on appelle r*isk data aggregation and risk reporting* (Basel Committee on Banking Supervision, 2012). Comme le veut l'adage : « les astres étaient alignés pour que ça arrive »… mais encore fallait-il avoir les moyens d'observer, voire de mesurer, cet alignement.

Le constat global issu du projet DOMINO permet de poser l'hypothèse générale qu'**une organisation qui met de l'avant la GIR pourra tirer profit de la mise en commun des ICII sur les risques qui sont réparties entre les différentes UF responsables des AGR afin d'obtenir une vision plus holistique des risques auxquels elle est confrontée et ainsi mieux supporter ses processus de prise de décisions plus tactiques et stratégiques relatifs à leur gestion.** Le défi pour les grandes organisations est donc de parvenir à faire en sorte que toutes les UF responsables des AGR puissent travailler ensemble à mettre en commun leurs ICII sur les risques afin d'en tirer une connaissance collective à plus forte valeur ajoutée. Or, comme il l'a été montré dans l'article sur les défis liés à la gestion des risques émergents, lorsque plusieurs parties prenantes sont impliquées dans la même entreprise, une solide gouvernance doit être établie afin de s'assurer que chacune d'elles comprenne bien ses rôles et ses responsabilités (et celles des autres) dans l'entreprise commune et, surtout, afin de s'assurer de la coordination, la complémentarité et la cohérence des décisions qu'elles prennent et des actions qu'elles posent. Ce projet de recherche s'intéressera donc à définir cette gouvernance liée à la GIR. Ainsi, de l'hypothèse générale découle la question de recherche à laquelle tentera de répondre ce projet : **Est-il possible de développer un cadre de gouvernance complet et opérationnel pour la GIR qui permettra aux grandes organisations de mieux agréger les ICII sur les risques et de générer des connaissances collectives nouvelles et transdisciplinaires leur permettant de mieux supporter leurs processus de prise de décisions plus tactiques et stratégiques quant aux risques à gérer ?**

Pour répondre à cette question, l'hypothèse spécifique à la base de ce projet de recherche est qu'**il est possible de transposer le concept d'EC développé par le CRP dans le cadre du projet DOMINO aux grandes organisations pour qu'il prenne la forme d'un cadre de gouvernance pour la GIR.** Cette hypothèse a été suggérée lors de la rétrospective du projet DOMINO et repose sur le fait que la structure fonctionnelle des grandes organisations fait en sorte que les multiples UF au sein de l'organisation agissent, à l'instar des IC de l'EC, comme de nombreuses entités relativement indépendantes dans leur fonctionnement interne, même si fortement interdépendantes

dans leur fonctionnement collectif. Ainsi, même si elles ont chacune leurs objectifs et leurs façons de faire, ces UF ont toutes un rôle à jouer et contribuent toutes, à des degrés possiblement différents selon le contexte, à l'atteinte de la mission de l'organisation – tout comme les IC contribuent toutes, aussi à des degrés possiblement différents selon le contexte, au bien-être et au bon fonctionnement de la société. Or, même si elles appartiennent toutes à la même organisation, il y a souvent peu de communication entre ces UF, ou si elle existe, celle-ci n'est pas nécessairement formalisée et encadrée (comme c'est le cas aussi pour les communications entre les IC). Or, cette communication est absolument essentielle pour aborder les problématiques transverses, c'est-à-dire les problématiques ou questions complexes, aux multiples dimensions, qui traversent différents domaines, disciplines, compétences, départements, secteurs ou organisations et qui nécessitent une approche de résolution plus holistique (Ministère de l'Éducation du Québec, 2006). Cette analogie entre les IC d'un environnement socio-économique et les UF d'une grande organisation est présentée à la figure 4.1.

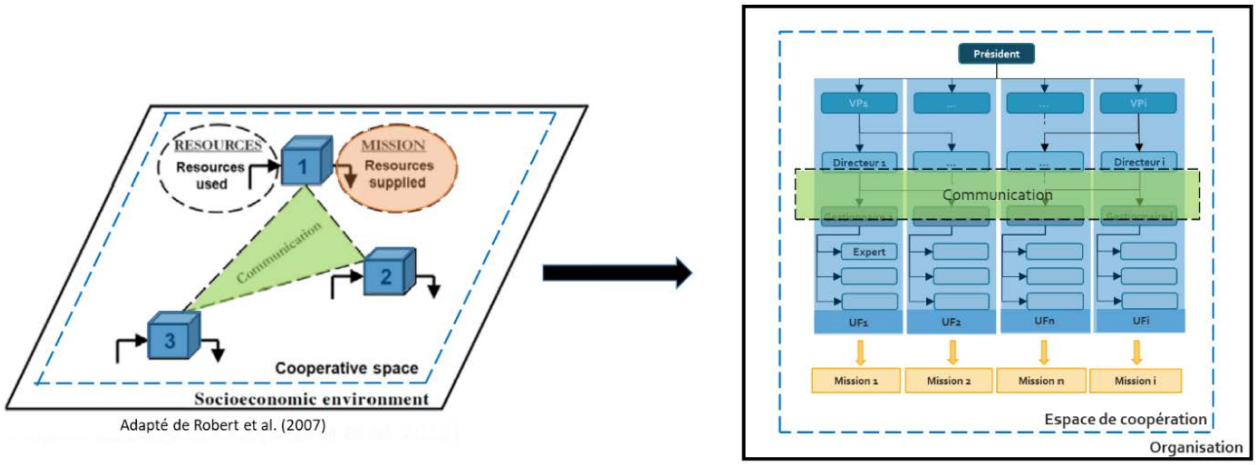


Figure 4.1 Analogie entre les IC d'un environnement socio-économique et les UF d'une grande organisation

Évidemment, dans le cadre de ces travaux de recherche, les UF responsables des AGR sont les principales concernées. La section suivante visera à traduire la question de recherche et son hypothèse spécifique en objectifs de recherche à atteindre.

4.2 Objectifs de recherche

4.2.1 Objectif général

L'objectif général de ce projet de recherche découle de la question de recherche et consiste à développer un cadre de gouvernance complet et opérationnel pour la GIR chez les organisations de grande ampleur. L'implémentation de ce cadre de gouvernance dans une grande organisation devra permettre à cette dernière de générer des connaissances collectives nouvelles et transdisciplinaires lui permettant de mieux appuyer ses processus de prise de décisions plus tactiques et stratégiques en regard des risques, ce que vise précisément la mise en place du cadre de gouvernance pour la GIR qui est proposé dans cette thèse.

Ainsi, quelques conditions devront donc être remplies afin de prouver l'atteinte de l'objectif général de ce projet de recherche. Premièrement, le cadre de gouvernance devra être considéré comme étant complet. Par complet, on entend que le cadre de gouvernance inclut l'ensemble des éléments clés de la gouvernance tels que présentés à la figure 3.3. Rappelons que ces éléments clés de la gouvernance ont été établis en fonction des constats issus de la revue de la littérature du concept de gouvernance effectuée principalement par Lacroix et St-Arnaud (2012) et qui a été présenté à la section 3.6.2. Ensuite, le cadre devra être considéré comme étant opérationnel. Par opérationnel, on entend que l'implémentation du cadre de gouvernance dans une grande organisation est réalisable et réaliste. Dans le cadre de ces travaux de recherche, il s'agira donc de vérifier que le cadre a effectivement pu être implémenté dans une grande organisation et que cette implémentation porte raisonnablement à croire qu'il puisse être implémenté dans d'autres grandes organisations. Finalement, le cadre devra permettre aux différentes UF responsables des AGR de mettre en commun leurs ICII sur les risques et de générer des connaissances collectives nouvelles et transdisciplinaires permettant à l'organisation de mieux appuyer ses processus de prise de décisions plus tactiques et stratégiques en regard des risques. En ce sens, le cadre devra créer de la valeur pour l'organisation qui le met en place en lui permettant de générer des connaissances sur les risques qu'elle ne pourrait générer autrement que par une coopération accrue entre les UF responsables des AGR. Rappelons que la création de valeur, comme il l'a été montré au chapitre 2, est une condition essentielle au succès et à la pérennité de toute coopération.

4.2.2 Objectifs spécifiques

Les objectifs spécifiques de ce projet de recherche découlent de l'hypothèse spécifique de recherche. Celle-ci suggère qu'il est possible de transposer le concept d'EC afin qu'il prenne la forme d'un cadre de gouvernance pour la GIR chez les organisations de grande ampleur. Pour valider cette hypothèse, il est donc nécessaire d'identifier les principales composantes (ou caractéristiques) d'un EC et voir comment celles-ci pourront être transposées au contexte de la GIR chez les grandes organisations. Les sections suivantes présentent ces composantes d'un EC.

4.2.2.1 Un référentiel commun pour les entités coopérantes

L'EC repose sur l'existence d'une problématique commune aux organisations prenant part à la coopération et dont la résolution dépasse le cadre de fonctionnement d'une seule organisation. À cet égard, la difficulté réside dans l'établissement de la vision commune (ou RMC) de cette problématique par l'ensemble des parties prenant part à la coopération. La RMC est essentielle afin de s'assurer que toutes les parties prenantes aient la même vision de la problématique à résoudre et travaillent en synergie vers sa résolution (donc, vers l'atteinte de l'objectif commun).

Dans le cadre du projet DOMINO, la problématique commune aux IC ayant pris part au projet de recherche était les interdépendances entre elles. Ces interdépendances étaient dues aux échanges de ressources entre les IC et avaient été schématisées par une figure de Rinaldi et al. (2001) qui allait devenir emblématique de cette problématique et qui est présentée à la figure 4.2. Cette figure devenait donc la RMC de la problématique des interdépendances entre les IC qui devait être résolue.

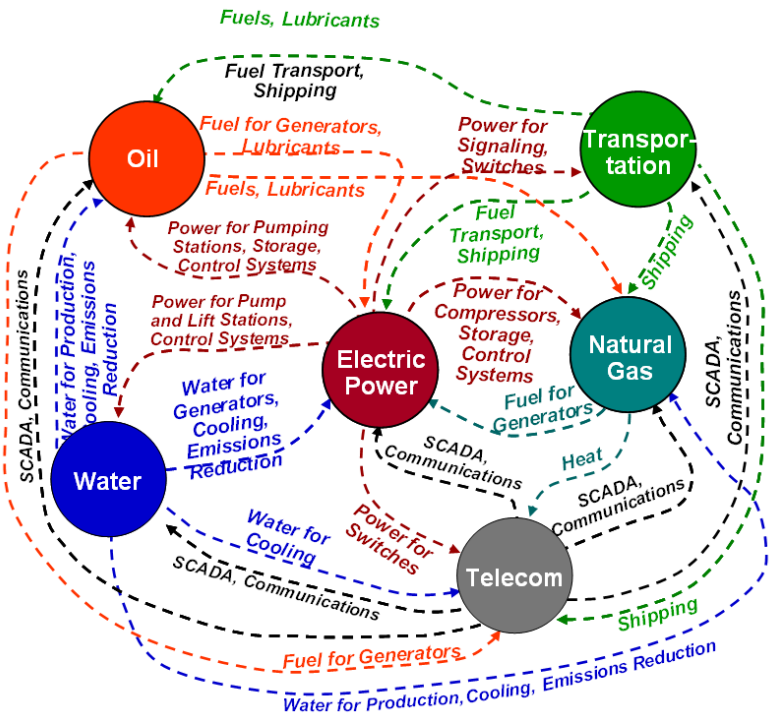


Figure 4.2 Représentation des interdépendances entre les IC (Rinaldi et al. 2001)

Pour aborder cette problématique, le CRP allait traduire cette image sous une forme beaucoup plus facile à conceptualiser. Celle-ci est illustrée à la figure 4.3.

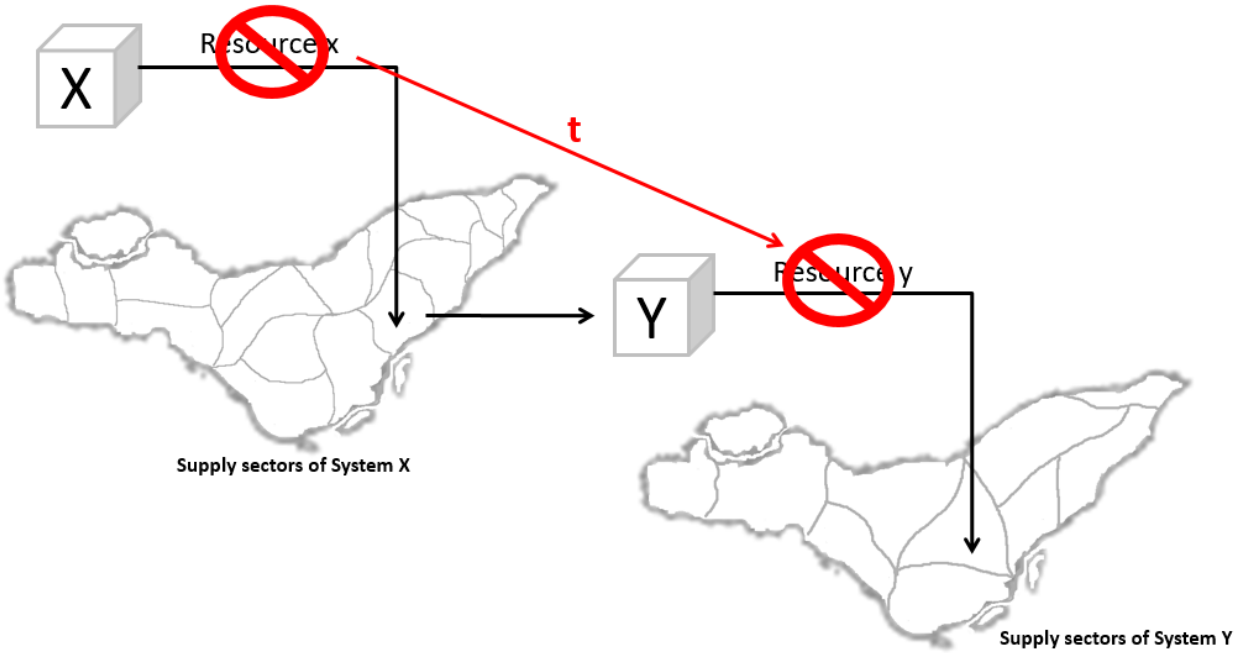


Figure 4.3 RMC de la problématique des interdépendances entre les IC (Robert et Morabito, 2010b)

Pour traduire cette figure en mots, chaque IC d'un environnement socio-économique a pour mission de fournir, dans cet environnement, une ressource qui est utilisée par les autres IC pour fournir leur propre ressource. Une dégradation de l'une ou l'autre de ces ressources dans un secteur de l'environnement peut donc se répercuter sur les autres IC et compromettre, après un certain temps, leur capacité à fournir leur propre ressource dans un secteur (ou plusieurs) de l'environnement, engendrant ainsi un phénomène d'effet domino. L'analyse de chaque lien de dépendance entre les différentes infrastructures appartenant aux IC présentes à Montréal et la mise en commun des résultats de ces analyses allaient donc permettre de dresser le portrait des interdépendances entre les IC sur le territoire montréalais et répondre à la problématique illustrée par la figure 4.2.

Ainsi, au niveau de ce projet de recherche, **le premier objectif spécifique consistera à établir le référentiel commun aux UF responsables des AGR.** Ce référentiel commun devra fournir aux acteurs au sein de ces UF une RMC de la problématique de la GIR qui leur permettra de clairement visualiser à quels niveaux se situe leur implication dans cette problématique à résoudre. Pour faire le parallèle avec les figures 4.1 et 4.3, il s'agit donc de comprendre comment leur mission est liée à la problématique. Le référentiel commun constituera le premier pilier du cadre de gouvernance pour la GIR chez les organisations de grande ampleur proposé dans cette thèse.

4.2.2.2 Une structure de coopération favorisant les échanges entre les organisations coopérantes

L'EC repose sur une structure de coopération misant sur la présence d'un animateur neutre et compétent afin de favoriser les échanges d'informations entre les organisations coopérantes. La figure 4.4 montre la structure de coopération mise sur pied dans le cadre du projet DOMINO.

Figure 4.4 Structure de coopération du projet DOMINO (Morabito et Robert, 2015)

Dans cette structure, le comité directeur était composé de dirigeants provenant de chacune des organisations partenaires et du directeur du CRP. Ce comité avait pour but de fixer les grandes orientations et les grands objectifs de la coopération, d'assurer le bon avancement des travaux en regard de l'atteinte de ces objectifs et d'assurer le bon fonctionnement de la coopération en y dédiant les ressources nécessaires et en gérant le volet bureaucratique de la coopération (ententes contractuelles, ententes de non-divulgation, etc.). Le comité technique était quant à lui composé de représentants des organisations partenaires ainsi qu'un représentant du CRP (l'expert technique, en l'occurrence, l'auteur de ces lignes). Les représentants des organisations étaient responsables de fournir les informations sur les ressources que leur organisation utilisait dans les différents secteurs de l'environnement socio-économique et sur les conséquences de la dégradation de ces ressources sur la capacité de leur organisation à fournir sa propre ressource (exprimées en termes de délais avant la défaillance de cette ressource, comme le montre la figure 4.3). L'expert technique avait pour rôle d'agréger et de corréler les informations fournies par les organisations partenaires et de les traduire sous la forme de courbes de dépendances comme celle illustrée à la figure 2.2. Finalement, l'animateur de l'EC était le CRP. Ce dernier avait pour rôle de guider les organisations vers l'atteinte des objectifs de la coopération en fournissant l'expertise relative aux interdépendances et en assurant la logistique du fonctionnement de la coopération (demandes de subvention, gestion des livrables, planification des rencontres, etc.).

Ainsi, au niveau de ce projet de recherche, **le deuxième objectif spécifique consistera à établir la structure de coopération qui supportera le cadre de gouvernance pour la GIR.** Or, contrairement au projet DOMINO où la structure de coopération était mise sur pied dans le cadre d'un projet (donc, caractérisé par un début et une fin) et opérait à l'extérieur des organisations partenaires, celle développée pour la GIR devra être pensée pour opérer en continu (donc, de manière pérenne) et à l'intérieur de l'organisation partenaire. Le défi consistera alors à déterminer la forme que devra prendre cette structure de coopération et comment elle pourra s'intégrer à la structure organisationnelle fonctionnelle afin de créer un arrimage harmonieux. La structure de coopération constituera le second pilier du cadre de gouvernance pour la GIR chez les organisations de grande ampleur proposé dans cette thèse.

4.2.2.3 Un modèle d'agrégation des informations et des connaissances

L'EC repose sur le principe que chaque organisation demeure propriétaire de ses informations. Seuls les résultats des analyses effectuées à l'interne des organisations sont partagés. Dans le cadre du projet DOMINO, les analyses de dépendances aux ressources étaient effectuées à l'interne par les organisations partenaires. Seuls les résultats de ces analyses, une fois traduites par le CRP sous la forme de courbes de dépendances comme celle illustrée à la figure 2.2, étaient communiqués à l'EC. Ensuite, en fonction d'un scénario de défaillance quelconque, les courbes de dépendances pertinentes à l'analyse de ce scénario étaient agrégées pour générer la courbe d'effet domino associée à ce scénario. La figure 4.5 présente un exemple d'une telle courbe.

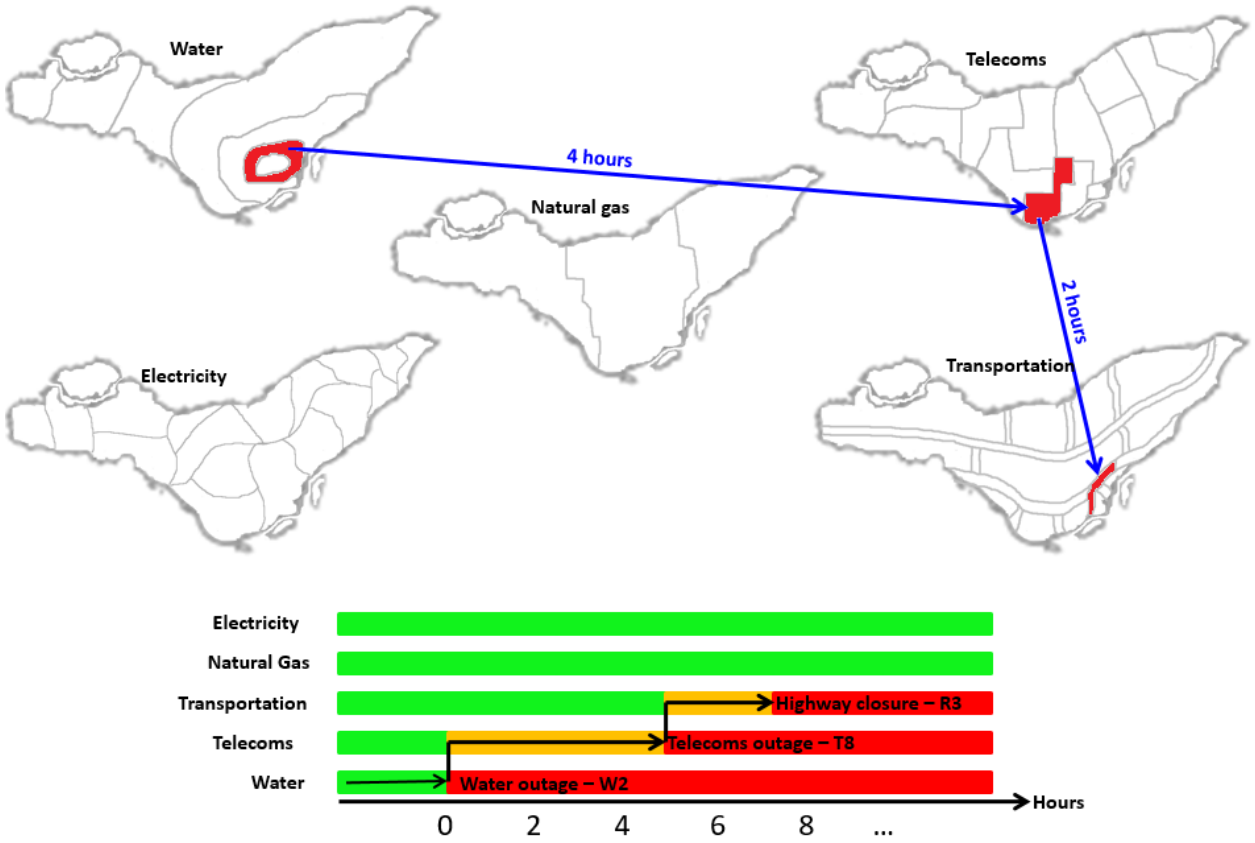


Figure 4.5 Exemple d'une courbe d'effet domino (Robert et Morabito, 2010b)

Dans cet exemple, une panne d'eau dans un secteur de l'environnement engendre une panne de télécommunications après 4 heures dans un autre secteur qui, à son tour, engendre la fermeture d'un axe routier majeur après 2 heures dans un autre secteur. La courbe d'effet domino permet alors de faire le lien entre une panne d'eau initiale dans un secteur de l'environnement et la fermeture d'un axe routier majeur, 6 heures plus tard, dans un autre secteur de l'environnement,

alors qu'*a priori*, rien ne semblait indiquer (ou laissait présupposer) un possible lien entre ces deux événements.

La valeur ajoutée de ces courbes résidait dans le fait qu'il devenait alors possible d'établir un lien géographique et temporel entre une défaillance d'une infrastructure (ou équipement) d'une IC et ses impacts directs sur d'autres infrastructures (ou équipements) appartenant à d'autres IC (effet domino de 1er ordre), mais également d'établir un lien entre des défaillances apparemment sans lien direct de cause à effet (effet domino de 2e ordre et plus). Ces connaissances nouvelles, qu'il n'aurait été possible de générer autrement que par la coopération entre les organisations partenaires et par la possibilité de combiner des informations à l'intérieur d'un référentiel commun, permettaient alors d'identifier des alignements de vulnérabilités potentiels et d'établir des plans particuliers d'intervention visant la résolution de ces situations potentiellement génératrices d'effets domino.

Ainsi, au niveau de ce projet de recherche, **le troisième (et dernier) objectif spécifique consistera à établir un modèle d'agrégation des ICII sur les risques qui sont réparties à travers l'organisation.** Cette agrégation devra produire des connaissances nouvelles à plus forte valeur ajoutée capables de mieux supporter les processus de prise de décisions plus tactiques et stratégiques relatifs aux risques à gérer. Le modèle d'agrégation des ICII sur les risques constituera ainsi le troisième (et dernier) pilier du cadre de gouvernance pour la GIR chez les organisations de grande ampleur proposé dans cette thèse.

4.3 Méthodologie de recherche

4.3.1 Fonctionnement général de la recherche

Ce projet de recherche sera conduit en deux volets menés en parallèle : un volet théorique et un volet pratique. Le volet théorique du projet s'intéressera à établir les concepts théoriques sur lesquels reposera le cadre de gouvernance pour la GIR chez les organisations de grande ampleur qui sera proposé dans cette thèse. Ainsi, les différents concepts théoriques associés à chacun des piliers du cadre de gouvernance seront abordés dans le cadre de ce volet du projet. Le volet pratique du projet s'intéressera quant à lui à opérationnaliser ces concepts théoriques en les traduisant en

outils concrets utilisables par les grandes organisations, permettant ainsi de s'assurer que le cadre développé est valide autant en théorie qu'en pratique.

Concernant le volet pratique, les travaux se feront en collaboration avec une grande organisation canadienne. Cette organisation, que l'on ne peut nommer par souci de confidentialité, est une grande organisation canadienne (la plus grande de son secteur d'activité) composée d'une dizaine d'unités d'affaires principales, plus de 45 000 employés et plus de 20 000 sites[9] répartis principalement au Canada, mais aussi aux États-Unis, au Maroc et en Inde. Plus précisément, les travaux se feront au sein de la direction « Sûreté et résilience de l'entreprise ». Cette direction couvre l'ensemble des unités d'affaires de l'organisation et regroupe quatre UF responsables de : (1) la continuité des affaires, (2) la gestion des accès, (3) la gestion des incidents et des mesures d'urgence et (4) la protection des actifs et la sécurité physique. Le volet pratique permettra de s'assurer que le cadre développé est bien opérationnel (en lien avec l'objectif général de recherche).

Pour assurer la bonne conduite du volet pratique du projet, une structure similaire à la figure 4.4 a été mise sur pied. Ainsi, une équipe de projet, que l'on pourrait associer au comité technique, composée de cinq experts provenant de chacune des UF a été formée. Ces experts auront pour tâche principale d'opérationnaliser les différents éléments du cadre de gouvernance qui seront développés dans le cadre du volet théorique du projet. Avec le chercheur, ces experts participeront donc à mieux cerner la problématique et la définir (au niveau pratique) ainsi qu'à développer les outils qui permettront d'opérationnaliser les concepts théoriques établis par la recherche et à les appliquer dans l'organisation. Ils devront donc partager avec le chercheur tout élément d'information pertinent relativement aux éléments du cadre de gouvernance qui fonctionnent bien et ceux qui fonctionnent moins bien afin de pouvoir apporter les correctifs nécessaires en cours de projet. Il est aussi attendu de ces personnes qu'elles partagent avec le chercheur toute information pertinente qui pourrait faire en sorte d'accroître la valeur ajoutée du cadre développé. Ces informations peuvent concerner des besoins spécifiques des UF, des problématiques particulières vécues ou des opportunités potentielles à saisir, par exemple.

Afin de suivre l'avancement du projet, un comité directeur a aussi été formé. Celui-ci est formé de la directrice, Sûreté et résilience de l'entreprise, ainsi que des gestionnaires de chacune des UF

[9] Par « site », on entend tout bâtiment pouvant abriter des actifs tangibles et intangibles comme du personnel, des équipements, des informations, etc.

présentes dans cette direction. Le comité directeur veillera à s'assurer que les travaux suivent bien leur cours, que les résultats produits cadrent bien avec les attentes et que les ressources dédiées au projet sont toujours suffisantes et, surtout, toujours motivées et engagées dans le projet.

4.3.2 Méthodologie de recherche

Pour orienter le choix de la méthodologie de recherche, il faut évidemment considérer le projet de recherche lui-même (donc, l'objet de la recherche), mais aussi la finalité recherchée et le contexte dans lequel le projet sera réalisé. Ainsi, ce projet de recherche vise à développer un cadre de gouvernance pour la GIR chez les organisations de grande ampleur. Ce cadre doit reposer sur des assises théoriques solides, mais il doit être opérationnel, c'est-à-dire qu'il doit pouvoir être utilisé en pratique, d'où l'intérêt de faire ce projet avec une organisation partenaire. Il y a donc clairement une forme de livrable qui est attendu de ce projet et qui consiste en la mise en place de ce cadre de gouvernance dans l'organisation partenaire. Ainsi, parmi l'éventail de méthodologies de recherche existantes, il importe d'en choisir une qui soit centrée sur les résultats (Réseau des Centres Collégiaux de Transfert de Technologie [RCCTT], 2023). De plus, comme ces travaux ne s'inscrivent clairement pas dans un contexte de recherche fondamentale où l'on cherche à développer de nouvelles connaissances théoriques sur un sujet donné, mais s'inscrivent plutôt dans un contexte où l'on cherche à employer et mettre ensemble des connaissances théoriques pour la plupart existantes, dans le but de fournir une solution novatrice à une problématique spécifique concrète, une méthodologie de recherche davantage appliquée est plus appropriée à ce contexte (RCTT, 2023).

Pour orienter davantage le choix de la méthodologie de recherche, il importe également de considérer comment le projet de recherche sera réalisé. Dans ce projet, le chercheur sera appuyé par des experts de l'organisation partenaire. Il importe donc de choisir une méthodologie qui tienne compte de cela, donc une méthodologie de recherche centrée sur la participation des acteurs, donc participative (Renaud, 2020). Dans ce type de méthodologie, les acteurs de terrain sont directement impliqués dans le processus de recherche et sont activement impliqués dans la co-construction des connaissances nécessaires à la réalisation du projet et à l'atteinte de ses objectifs (Renaud, 2020).

Finalement, dans le choix définitif de la méthodologie de recherche, il importe de considérer le rôle du chercheur. Dans le cadre de ce projet de recherche, le chercheur n'agira pas en tant qu'observateur d'une situation problématique à changer ou comme un consultant laissant la

responsabilité des actions au milieu preneur. Plutôt, il participera directement et activement au processus de transformation des acteurs et des façons de faire de l'organisation (Renaud, 2020 ; Roy et Prévost, 2013). Ainsi, en tenant compte de cette implication du chercheur dans la transformation (donc, dans le changement), la méthodologie de recherche la plus adaptée à ce contexte, et qui sera mise de l'avant dans le cadre de ce projet de recherche, est la recherche-intervention.

La recherche-intervention est une variante de la recherche-action. La principale différence entre les deux réside dans le fait que la recherche-action se concentre davantage sur les changements de comportements des acteurs de terrain alors que la recherche-intervention vise à transformer à la fois les comportements de ces acteurs et les structures mêmes de l'organisation dans laquelle ces changements s'opèrent (Renaud, 2020). Ainsi, l'objectif de la recherche-intervention est de conduire une action de transformation durable qui touche autant les pratiques individuelles des acteurs de terrain impliqués dans le déploiement de l'intervention que les conditions organisationnelles dans lesquelles s'inscrivent ces pratiques (Renaud, 2020). Pour cette raison, dans ce type de recherche, il s'avère nécessaire d'avoir un comité de suivi formé d'acteurs de terrain et de cadres de l'organisation, de même qu'un comité de projet interne constitué d'acteurs de terrain et de chercheurs, afin de légitimer la transformation (donc, le changement) (Renaud, 2020).

Au-delà de cette distinction, la recherche-action et la recherche-intervention partagent essentiellement les mêmes fondements et le même déroulement. Ainsi, la recherche-intervention, comme la recherche-action, constitue à la fois une méthode de recherche et une méthode de mise en oeuvre des changements (Roy et al. 2013). Les deux méthodologies prévoient que les membres du milieu preneur et les chercheurs collaborent à toutes les étapes du processus de recherche ainsi qu'à l'étude et à la génération des résultats qui en découlent (Renaud, 2020 ; Roy et al. 2013). En impliquant directement le milieu preneur dans les analyses, ces dernières sont plus ciblées et offrent des résultats qui sont plus concrets, plus fiables et qui répondent mieux aux besoins réels des parties prenantes qui sont alors plus enclines à s'en approprier les résultats au niveau organisationnel. De plus, comme il participe directement à l'identification des problèmes et à l'identification des solutions à mettre en place, le milieu preneur devient alors l'acteur principal au centre du changement, ce qui réduit énormément la résistance au changement (Roy et al. 2013 ; Roy et Prévost, 2013).

Au niveau de la démarche, la méthodologie de la recherche-intervention utilise essentiellement la même démarche cyclique de résolution de problème que la recherche-action. La figure 4.6 présente le cycle type de la démarche de recherche-action.

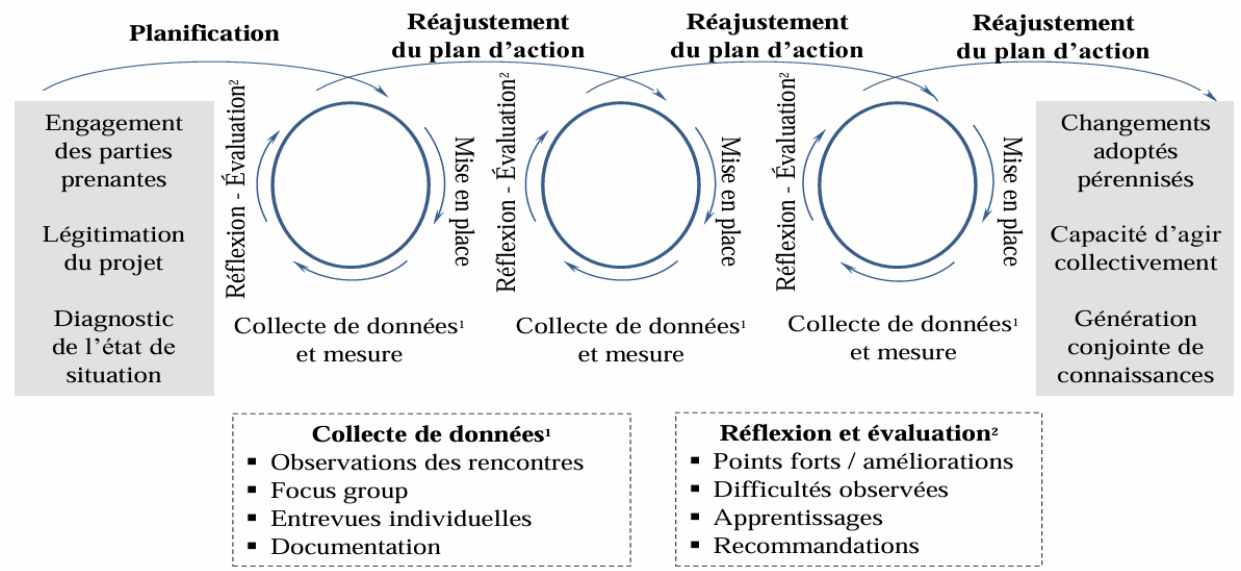


Figure 4.6 Cycle de la démarche de la recherche-action (Roy et Prévost, 2013)

Les sections suivantes présentent chacune des grandes phases de la démarche de la recherche-action et montrent plus concrètement comment celles-ci ont été mises en pratique au niveau des travaux de recherche présentés dans cette thèse.

4.3.2.1 La phase d'engagement des parties prenantes

La démarche de la recherche-action commence par une première grande phase d'engagement des parties prenantes. Comme son nom l'indique, cette phase vise à engager dans le projet de recherche l'ensemble des parties prenantes qui pourraient avoir une incidence sur le projet, donc, à les mobiliser et les rallier à la cause commune. Cet engagement est nécessaire afin de confirmer l'existence du projet de recherche, légitimer les actions qui seront prises sur le terrain par les membres de l'équipe de projet et maximiser les chances de succès du projet (Boivin et al., 2022 ; PMI, 2021). Selon le PMI (2021), la phase d'engagement des parties prenantes doit faire partie intégrante de la gestion de tout projet. Celle-ci doit comprendre un plan d'engagement qui inclut cinq grandes activités : (1) l'identification des parties prenantes, (2) l'analyse des parties prenantes, (3) le plan d'engagement des parties prenantes, (4) l'engagement des parties prenantes et (5) le

suivi de l'engagement. Des outils, comme la cartographie des parties prenantes et les matrices d'engagement des parties prenantes, sont aussi recommandés afin de mener à bien cette phase[10].

Dans le cadre des travaux menés avec l'organisation partenaire, le chercheur a d'abord consulté ses équivalents chez les autres UF responsables des AGR afin de s'enquérir auprès de ces personnes de leur perception quant à l'existence, ou non, d'un besoin d'une plus grande et formelle coopération entre eux et, plus spécifiquement, sur le besoin d'une plus grande intégration de leurs travaux. Ces discussions et échanges ont permis de confirmer ce besoin auprès de ces acteurs et, par le fait même, de valider leur intérêt et leur appui à participer à un éventuel projet de développement d'un cadre de gouvernance pour la GIR.

Suite à ces discussions, une première représentation pour la mise en place d'un projet-pilote visant à développer un cadre de gouvernance pour la GIR a été faite par le chercheur, auprès de la directrice, Sûreté et résilience de l'entreprise, au sein de l'organisation partenaire. Au cours de cette rencontre, le chercheur a dû expliquer la problématique associée au fonctionnement en silo des UF sous cette direction, mais, surtout, comment il comptait aborder cette problématique par le biais du développement d'un cadre de gouvernance pour la GIR et quelles seraient les retombées positives potentielles de la mise en place d'un tel cadre. Cette représentation a eu lieu en janvier 2020 avec un accueil favorable à la mise en place éventuelle d'un projet-pilote permettant de conduire cette initiative[11]. Cependant, ce n'est qu'en avril 2020, qu'une nouvelle représentation a eu lieu, à la demande de la directrice, Sûreté et résilience de l'entreprise, cette fois. Cette représentation a été faite auprès des gestionnaires des UF responsables des AGR sous cette direction[12]. Suivant cette

---

[10] L'engagement des parties prenantes est pratiquement devenu un domaine de recherche en soi. Or, il n'est pas dans l'objectif de cette thèse d'élaborer sur cette phase de tout projet. Néanmoins, il est fortement recommandé à quiconque voudrait lancer une initiative similaire d'effectuer une recherche sur le sujet afin de ne pas rater cette phase cruciale. Si la phase d'engagement n'est pas conduite adéquatement, les chances de succès d'obtenir un projet et, éventuellement, de le mener à bien, sont drastiquement réduites.

[11] La première représentation auprès de la personne (ou le groupe de personnes) qui a l'autorité de donner l'aval au projet doit être préparée avec beaucoup de soins. Cette représentation ne doit pas avoir pour objectif de critiquer négativement ce qui est fait dans l'organisation, mais plutôt de mettre l'emphase sur ce qui pourrait venir bonifier ce qui se fait de bien déjà dans l'organisation. L'emphase doit donc être mise sur les solutions, au détriment des problématiques et des enjeux. La représentation doit être basée sur des faits. Des exemples concrets, des figures, des tableaux et des chiffres doivent venir appuyer les propos tenus lors de cette rencontre. Surtout, pour l'instigateur de l'initiative, il s'agit de rassurer son interlocuteur et de démontrer qu'il possède les compétences, les connaissances, l'expertise et le leadership nécessaire pour conduire et mener à bien le projet.

[12] Entre la première représentation en janvier 2020 et la deuxième, en avril 2020, la première vague de la pandémie de COVID-19 frappait durement partout autour du globe et un confinement général avait été décrété au Québec et ailleurs au Canada. Les enjeux que soulevait la gestion de cet événement venaient alors clairement mettre en lumière les propos du chercheur tenus lors de la première représentation et venaient aussi démontrer sans équivoque le besoin pour une gestion des risques plus intégrée au niveau de l'organisation partenaire. Ces événements, que l'on pourrait qualifier de « ruptures créatrices » (Lagadec, 2000) sont des opportunités de changements qui, lorsqu'elles surviennent au moment propice, doivent être saisies.

rencontre, la directrice et les gestionnaires des UF ont donné leur aval officiel au projet de recherche et ont identifié les experts au sein de leurs équipes qu'ils croyaient les plus aptes à travailler sur ce projet. Ces experts ont été judicieusement sélectionnés en fonction de leur grande expertise, leurs compétences et leurs connaissances de leur domaine d'activités. Cependant, comme ces personnes n'allaient pas être dégagées de leurs tâches régulières durant le projet, la décision finale de participer ou non au projet de recherche leur était laissée. Si aucun de ces experts n'avait souhaité participer au projet, celui-ci n'aurait probablement pas eu lieu. Pour cette raison, il importe, avant-même la première représentation auprès des décideurs, de consulter ces personnes pour « sonder le terrain » et avoir une forme de préapprobation de ces experts de leur engagement éventuel à participer au projet. Ce sondage préalable du terrain est fortement recommandé avant d'entreprendre toute forme de représentations plus formelles pour éviter un investissement inutile de temps et d'énergie (si les personnes ne démontrent aucun intérêt envers le projet).

Afin de sceller le mandat de ce projet de recherche et légitimer les travaux qui lui sont inhérents, une charte de projet[13] a été créée par le chercheur et l'équipe de projet, approuvée par le comité directeur et signée par la directrice, Sûreté et résilience de l'entreprise. La charte de projet comprenait un énoncé de la problématique à traiter, la portée, la durée et les coûts estimés du projet, les échéanciers ainsi que les livrables attendus, les risques anticipés et les ressources humaines qui allaient y participer. La création de la charte de projet est essentielle dans tout projet, mais tout spécialement dans le cadre de travaux, comme ceux présentés dans cette thèse, qui sortent du cadre des opérations courantes de l'organisation. En effet, non seulement la charte de projet permet de s'assurer que toutes les parties prenantes ont la même vision du but et des objectifs du projet, mais elle se veut aussi un point de référence important permettant de recentrer le projet sur ses objectifs périodiquement et au besoin. Dans un contexte où les personnes qui sont affectées au projet conduisent plusieurs autres initiatives en parallèle et où le projet est prévu s'échelonner sur quelques années, et qu'au cours de ces années plusieurs changements organisationnels peuvent survenir, la charte de projet devient un élément incontournable.

[13] La charte de projet ayant été classifiée comme étant « confidentielle » par l'organisation partenaire, il n'a pas été possible d'en inclure une copie, même caviardée, en annexe de cette thèse.

4.3.2.2 La phase de recherche

Le coeur de la démarche de la recherche-action est constitué d'un cycle itératif d'actions au cours desquelles les acteurs de terrain et le chercheur travaillent ensemble à identifier et planifier des stratégies pour améliorer la situation (planification/ajustement), à mettre en oeuvre ces stratégies (action/mise en place), à mesurer les effets de ces stratégies sur la situation (collecte de données/mesure) et à évaluer les effets de ces stratégies sur la situation (réflexion/évaluation). Ce cycle se répète jusqu'à ce que les parties prenantes soient satisfaites de la solution trouvée à la problématique et des apprentissages collectifs effectués.

Afin de mener à bien cette phase, il est fortement recommandé de prévoir plusieurs types de rencontres avec les parties prenantes impliquées afin d'aider au tissage des liens entre les individus et à la co-construction des connaissances collectives. À cet effet, il existe plusieurs types de rencontres différentes, chacune visant des objectifs différents, que ce soit des rencontres d'informations, des séances de remue-méninges ou d'idéation, des séances de travail de groupe ou des séances de travail individuel ou en comité restreint ou des réunions de suivi[14], par exemple. Il importe donc de sélectionner les types de rencontres appropriées à l'atteinte des différents objectifs du projet (Mongeau et Saint-Charles, 2024) et de prévoir celles-ci à la charte de projet.

Dans le cadre des travaux avec l'organisation partenaire, le chercheur et l'équipe de projet se sont réunis à raison d'une fois par semaine lors de réunions de travail de groupe d'une heure[15]. Au tout début des travaux, ces réunions avaient pour objectif principal de permettre aux différents acteurs de se connaître, d'abord personnellement, afin de commencer à établir un lien de confiance mutuelle, et ensuite professionnellement, afin d'en apprendre davantage sur leurs expertises et leurs rôles et responsabilités au sein de leur UF respective. Ensuite, des réunions prenant la forme de séances de formation ont eu lieu. Pour le chercheur, ces réunions visaient à former les experts au

[14] La littérature regorge de documents qui abordent les réunions de travail. Encore ici, il n'est pas dans l'objectif de cette thèse d'élaborer sur ce sujet, mais il est fortement recommandé pour quiconque voudrait reprendre un projet de recherche similaire, ou tout autre projet de recherche faisant appel à la méthodologie de la recherche-intervention, d'effectuer quelques recherches préalables sur le sujet afin de bien identifier les types de réunions qui cadrent le mieux avec les objectifs poursuivis.

[15] Le contexte pandémique et le fait que les membres de l'équipe étaient dispersés dans différentes provinces canadiennes faisaient en sorte que ces réunions se faisaient en mode virtuel, amenant ainsi une difficulté supplémentaire relativement à la création des liens interpersonnels entre les membres de l'équipe. Ainsi, pour compenser cette difficulté, il faut permettre aux membres de l'équipe de mieux se connaître et de parvenir à tisser des liens, malgré la distance. Pour cela, on doit laisser de la place, durant les réunions officielles ou à l'extérieur des réunions officielles, aux échanges plus informels et plus personnels concernant les personnes, leur famille, leurs loisirs ou simplement pour discuter de tout et de rien ou de l'actualité. Si les réunions ne visent que le projet, alors on risque de passer à côté de l'un des objectifs fondamentaux de la GIR qui consiste aussi à créer une cohésion entre les acteurs.

niveau des concepts de risque traditionnel, de risque émergent, de gestion des risques et de GIR et au niveau de ce qui était recherché par la mise en place d'un cadre de gouvernance pour la GIR ; pour les experts des UF responsables des AGR, ces réunions visaient à présenter leur domaine d'expertise aux autres membres de l'équipe de projet, à leur offrir (ainsi qu'au chercheur) une formation de base leur permettant de comprendre globalement la nature des activités conduites par leur UF respective et de se familiariser avec leur domaine d'activité et le vocabulaire employé. Toutes ces réunions avaient pour objectifs d'établir une base de connaissances commune aux membres de l'équipe, d'adopter un langage commun et d'établir une vision commune de l'ensemble de la problématique à résoudre. Les réunions de travail subséquentes, davantage des séances de travail, de remue-méninges et d'idéation, ont porté plus spécifiquement sur le développement du cadre de gouvernance pour la GIR lui-même (et ses trois piliers) et des outils qui lui sont associés. Au-delà des réunions hebdomadaires, du temps de travail individuel (évalué à environ trois heures par semaine) était aussi prévu pour que chaque expert puisse travailler à produire les livrables associés au projet. Évidemment, en tout temps, il était possible pour les différents acteurs de planifier des rencontres individuelles ou en comité restreint pour discuter de sujets particuliers ou pour obtenir des précisions à des questions ou des problématiques spécifiques.

D'autres réunions, entre le chercheur et le comité directeur du projet cette fois, avaient lieu à raison de 15 minutes, une fois par mois et à raison de 30 minutes, deux fois par année. Ces réunions de suivi visaient à présenter les grands résultats livrés par le projet et à présenter les travaux qui allaient suivre. Ces réunions permettaient, d'une part, de constater l'avancement du projet, de faire état des apprentissages nouveaux effectués et des recommandations faites par les experts participants au projet quant aux améliorations possibles souhaitées et, d'autre part, d'adresser toute question pertinente requérant une décision du comité directeur.

Concernant le volet plus théorique de la recherche, des réunions de travail et de suivi entre le chercheur et le directeur de recherche avaient lieu périodiquement, à raison de deux heures par deux semaines. Concernant le temps personnel investi par le chercheur dans ce projet de recherche, celui-ci n'a pas été officiellement comptabilisé, mais une trentaine d'heures par semaine (en moyenne) de travail individuel de recherche ont été consacrées au projet de recherche en plus du temps consacré aux réunions de travail et de suivi planifiées.

4.3.2.3 La phase de clôture

La démarche de la recherche-action se clôt par une mise en oeuvre des changements et une pérennisation de ces changements au sein de l'organisation. Assurer le caractère pérenne des changements est un défi en soi puisque les organisations changent constamment et les individus, au sein de ces organisations, changent aussi. Dans le cadre d'un projet de recherche comme celui présenté dans cette thèse qui vise la construction de connaissances nouvelles, la pérennisation des résultats de la recherche, outre que ceux faisant l'objet des publications scientifiques, peut aussi représenter un défi particulier supplémentaire puisque ceux-ci peuvent être « attachés » aux individus par le biais de nouvelles connaissances qui sont davantage tacites. L'objectif est donc de traduire ces connaissances tacites en connaissances explicites. L'une des manières d'y parvenir consiste à intégrer ces changements aux façons de faire de l'organisation ou à la structure de l'organisation afin qu'ils s'intègrent à la culture organisationnelle. Selon l'ampleur du changement, une stratégie de gestion du changement doit également être mise en place et une période de transition (d'ajustements) doit aussi être prévue afin que tous les acteurs concernés par le changement puissent avoir le temps d'assimiler les nouvelles façons de faire et modifier leurs routines comportementales en conséquence. Des formations doivent aussi être planifiées, au besoin, pour les acteurs concernés (Stripe, 2024)[16].

Dans le cadre des travaux avec l'organisation partenaire, certains changements requis identifiés au cours des travaux ont été inclus à des directives et des procédures existantes et certains autres ont été traduits sous la forme de directives et de procédures nouvelles. Ces changements font donc maintenant partie intégrante de la documentation organisationnelle, ce qui contribuera à assurer que les connaissances nouvelles issues de la recherche fassent désormais partie des façons de faire de l'organisation. Aussi, comme la documentation au sein de l'organisation partenaire fait l'objet d'un suivi régulier et d'une mise à jour périodique, cela contribuera à assurer le maintien à plus long terme d'une bonne partie des apprentissages qu'auront permis ces travaux de recherche.

[16] La gestion du changement est un domaine de recherche en soi. Or, il n'est pas dans l'objectif de cette thèse d'élaborer sur ce sujet. Néanmoins, il est recommandé de réfléchir aux types de changements que le projet de recherche vise afin de déterminer quel modèle de gestion du changement pourrait être le plus adapté au contexte puisqu'il en existe plusieurs (modèle de Kotter, modèle de Lewin, modèle de Bridges, modèle de Kübler-Ross, modèle ADKAR (*Awareness, Desire, Knowledge, Ability, Reinforcement*), modèle des 7S (*Strategies, Structures, Systems, Shared values, Skills, Style of management, Staff*), etc. Un plan de changement détaillé pourrait être requis (et bénéfique) selon le type et l'ampleur du changement (Stripe, 2024).

CHAPITRE 5 REVUE DE LA LITTÉRATURE

L’article sur les défis liés à la gestion des risques émergents présenté au chapitre 3 a permis de mieux comprendre les différences qui existent entre le risque traditionnel et le risque émergent. Ainsi, alors que le premier repose sur le concept d’espérance mathématique issue des sciences exactes et suppose donc que l’ensemble des paramètres du risque sont connus, le second repose sur le concept d’incertitude et suppose plutôt que le risque naît d’un manque de connaissances (donc, que l’ensemble des paramètres du risque ne sont pas connus). L’article a aussi permis de mieux comprendre les différences qui existent entre la gestion des risques traditionnelle et la GIR. Ainsi, alors que la gestion des risques traditionnelle fait davantage référence à un processus, comme celui proposé par la norme ISO31000 (ISO, 2018), la GIR fait plutôt référence à la notion de gouvernance liée aux risques (IRGC, 2005), c’est-à-dire à la répartition des rôles et des responsabilités des acteurs en lien avec la gestion des risques, à la coordination de ces acteurs (de leurs décisions et leurs actions) et à la mise en commun de leurs ICII sur les risques.

Cela ayant été établi, l’objectif de cette revue de littérature n’est pas de revenir sur ces concepts de risques émergents et de GIR, mais plutôt d’obtenir une vue d’ensemble de ce que l’on pourrait qualifier d’ « éléments d’intérêt » qui sont disponibles aux organisations qui voudraient mettre en place la GIR, c’est-à-dire d’éléments qui traitent de la GIR, mais dans son champ d’application pratique. Ainsi, parmi les principaux éléments d’intérêt qui émergent lors d'une recherche sur la GIR, on trouve principalement des outils, des normes et des standards, des cadres de gestion des risques, ainsi que des politiques, des guides et des lignes directrices.

Cette revue de la littérature abordera donc ces différents éléments et sera suivie d’une analyse critique afin d’identifier les principaux points à considérer lors du développement du cadre de gouvernance pour la GIR et qui sont, ou ne sont pas forcément, pris en compte par les éléments d’intérêt existants. Cette analyse permettra d’orienter la suite des travaux de recherche et, en définitive, permettra de mieux apprécier l’originalité de la solution proposée dans cette thèse en regard de l’existant.

5.1 Les outils

L'un des premiers constats que l'on fait en effectuant des recherches sur la GIR est que de nombreux liens renvoient vers des sites d'organisations offrant des services de consultation en gestion des risques. Plusieurs de ces organisations proposent aussi des outils qu'il suffit d'installer pour mettre en oeuvre la GIR[17]. Tous ces outils sont certainement très intéressants, mais cette revue de la littérature ne s'y attardera pas en détail. D'abord, parce que ces organisations ne décrivent pas leurs modèles et leurs approches, mais surtout, et fondamentalement, parce que la problématique de la GIR ne se résume pas à l'installation d'un outil informatique – tout comme la problématique des interdépendances entre les IC ne se résumait pas non plus à l'installation d'un outil informatique. En effet, comme il l'a été démontré au chapitre 3, la GIR est avant tout une problématique de gouvernance. Ainsi, avant même de penser à un outil informatique, une organisation doit d'abord répondre à plusieurs questions de nature plus fondamentale relativement à la manière dont elle gère les risques (ou voudrait les gérer). L'organisation partenaire dans ce projet possède d'ailleurs elle-même plus d'un de ces outils, mais ceux-ci demeurent peu utilisés. En effet, un point négatif de ces outils est que, tout comme la nature, ils ont horreur du vide. Laisser des champs vides dans ces outils fait en sorte que ceux-ci n'arrivent pas nécessairement à fournir les extrants pour lesquels ils ont été programmés. Ainsi, la prémisse sur laquelle ces outils sont conçus suppose que toutes les données sur les risques sont existantes, disponibles et préformatées d'une certaine manière, ce qui n'est pas toujours le cas dans les organisations, surtout lorsqu'on aborde la question des risques émergents pour lesquels certaines informations sont pratiquement inexistantes. De plus, ces outils sont configurés de manière assez générale afin de permettre une utilisation « standardisée » par le plus grand nombre d'organisations. Un énorme travail d'adaptation doit donc être effectué pour configurer ces outils en fonction de la réalité de l'organisation. Or, plutôt que de s'investir réellement dans la GIR, de revoir leurs façons de faire et leur culture organisationnelle en lien avec la gestion des risques, beaucoup d'organisations font le contraire de ce qui devrait être fait : elles tentent d'adapter leurs façons de faire aux outils. Or, comme le confirme l'étude de Jean-Jules et Vicente (2020), les organisations qui abordent la GIR comme un projet de mise en place d'un outil informatique vivent des frustrations profondes et se heurtent à des difficultés majeures ou n'y arrivent tout simplement pas puisque plusieurs étapes

[17] Le site Capterra propose plusieurs outils : https://www.capterra.com/integrated-risk-management-software/.

préalables n'ont pas été réalisées. Paradoxalement (ou ironiquement), ces étapes demanderaient de mettre en place un cadre de gouvernance pour la GIR. Le problème n'est donc pas nécessairement dans les outils eux-mêmes, mais plutôt dans la perception (ou l'illusion) que ces outils offriront des résultats rapides et compenseront les faiblesses de l'organisation que ce soit en termes de gouvernance, de connaissances ou de compétences, alors que ce n'est pas le cas. Les outils peuvent certainement venir subséquemment, afin de fournir un support supplémentaire, mais pas l'inverse.

5.2 Les normes et les standards

Les normes et les standards sont un deuxième type d'éléments d'intérêt que l'on retrouve dans la littérature. À cet effet, la plupart des grandes organisations se rabattent sur des normes existantes lorsqu'il est question d'adopter un certain standard. Cela est bien entendu normal : premièrement, il n'est pas nécessairement dans la mission d'une grande organisation de commencer à développer ses propres standards et, deuxièmement, de tels standards ne seraient pas forcément reconnus de toute manière. Donc, les organisations s'alignent normalement sur des standards ou des normes existantes, bien établies et émises par des organismes de référence.

Ainsi, certaines AGR possèdent leurs propres normes et standards. Parmi ceux-ci, certains sont relatifs à l'environnement (ISO14001), d'autres à la sécurité de l'information (ISO27001, ISO27005), d'autres à la continuité des affaires (ISO22301), d'autres aux mesures d'urgence (National Fire Prevention Association [NFPA] NFPA1600) et encore d'autres à la gestion des actifs (ISO55000, ISO55001 et ISO55002), par exemple. Bien que ces normes et standards soient conçus pour minimiser les risques et soient largement utilisés par les organisations, incluant l'organisation partenaire dans ce projet, ceux-ci ne sont pas relatifs à la GIR. Ainsi, dans le cadre de cette revue de la littérature, ces normes et standards relatifs aux AGR ne seront pas analysés davantage[18].

En revanche, certaines normes sont directement liées à la gestion des risques. Parmi celles-ci, la norme ISO31000:2018 (dont le processus est illustré à la figure 3.1) (ISO, 2018) est très certainement la référence en la matière. Or, comme il l'a été montré au chapitre 3, cette norme est relative au processus de gestion des risques et ne concerne donc pas directement la GIR. De plus,

[18] Même s'ils ne sont pas analysés davantage dans cette revue de la littérature, cette thèse considère ces normes et standards comme des éléments très importants qui doivent faire partie intégrante d'un cadre de gouvernance pour la GIR. Ainsi, ceux-ci seront considérés au niveau du référentiel commun (chapitre 6).

malgré que la norme emploie la définition du risque qui est basée sur le concept d'incertitude, le processus lui-même, demeure basé sur le concept de risque issu des sciences exactes, et tient donc pour acquis que les personnes qui appliquent le processus auront accès à toutes les informations et connaissances sur les risques. Il semble donc y avoir un certain décalage entre la définition du risque employée dans la norme et le processus qu'elle préconise.

Sur le plan de la gouvernance, la norme ISO31000 mentionne effectivement que toutes les parties prenantes doivent être impliquées dans le processus de gestion des risques (lors de la phase de communication et consultation, qui s'applique à toutes les étapes du processus), mais elle ne propose pas une manière concrète d'impliquer ces parties prenantes. Aussi, la norme semble considérer que le processus de gestion des risques au sein des organisations est centralisé et donc, que toutes les parties prenantes participent au même processus, alors que ce n'est pas forcément le cas dans les grandes organisations où la gestion des risques est généralement scindée entre plusieurs UF distinctes ayant chacune leurs propres façons de faire et leurs propres processus qui varient selon leurs domaines d'activités. Par exemple, les risques environnementaux sont souvent abordés en utilisant le modèle du noeud papillon (Center for Chemical Process Safety [CCPS], 2018) ; les risques de sécurité physique ou de sécurité informatique sont normalement abordés en utilisant le modèle de défense en profondeur (Baker and Benny, 2014 ; United States Department of Homeland Security [US DHS], 2014) ; les risques associés aux défaillances des équipements ou à la sûreté de fonctionnement peuvent recourir à d'autres modèles ou techniques d'analyse de risques comme, par exemple, le modèle *What-if* (Reason et al., 2006) ou l'Analyse des Modes de Défaillance de leurs Effets et de leur Criticité (AMDEC) (Kélada, 1994). Ainsi, pour une organisation qui veut mettre en place la GIR, cette norme n'est en soi pas suffisante puisqu'elle est davantage orientée vers le processus de gestion des risques lui-même que vers la gouvernance entourant la mise en oeuvre et l'opérationnalisation du processus à l'échelle d'une organisation dans un contexte où plusieurs parties prenantes sont impliquées (et encore moins dans un contexte où plusieurs processus différents peuvent être impliqués).

Sur le plan technique, la norme ISO31010 (appartenant à la famille de la norme ISO31000) propose plusieurs techniques et méthodes d'appréciation des risques comme la méthode *Hazards and Operability Study* (HAZOP), les réseaux de Bayes, les analyses de Markov ou les simulations de Monte-Carlo, par exemple (ISO, 2019b). Or, ces approches sont très numériques et nécessitent

pour la plupart plusieurs données opérationnelles (ou statistiques) afin de produire des résultats qui convergent vers une solution relativement fiable. Elles sont donc valables pour les risques opérationnels, pour lesquels plusieurs de ces données et statistiques sont disponibles ou pour lesquels des modèles mathématiques assez fiables existent aussi, mais le sont moins pour les risques émergents pour lesquels très peu de données sont disponibles. En revanche, la norme propose aussi d'autres modèles qui peuvent être basés sur des approches semi-quantitatives comme les arbres des causes ou les arbres de conséquences. Ces approches sont intéressantes puisqu'elles peuvent être employées pour alimenter la réflexion des experts et les aider à analyser d'une part, les aléas potentiels pouvant affecter l'organisation et ses actifs (analyses des causes) et d'autre part, les conséquences potentielles de la défaillance de ces actifs sur l'organisation et sa mission (analyse des conséquences). Dans un contexte de risques émergents, ces approches doivent être privilégiées aux dépens des approches plus quantitatives comme celles mentionnées précédemment puisqu'elles amènent les experts à réfléchir d'abord sur tout ce qui peut (ou pourrait) affecter l'organisation sans égard aux données ou aux modèles mathématiques.

5.3 Les cadres de gestion des risques

Au-delà des outils et des normes, on retrouve aussi dans la littérature plusieurs cadres de référence pour la gestion des risques. Même si tous ne concernent pas spécifiquement la GIR, ceux-ci présentent un intérêt particulier puisqu'ils pourront tout de même servir de base de comparaison pour le cadre de gouvernance qui sera proposé dans cette thèse. Ceux-ci seront donc analysés beaucoup plus en profondeur.

Dans cette revue, seuls les quatre cadres les plus connus sont analysés[19] :

- L'*Enterprise risk management framework* du Committee of Sponsoring Organizations (COSO) (COSO, 2004) ;
- Le *Risk governance framework* de l'International Risk Governance Council (IRGC) (IRGC, 2017) ;

[19] Il existe une panoplie de cadres de référence en gestion des risques. Or, la plupart sont dérivés de la norme ISO31000 et adaptés au contexte spécifique pour lequel ils sont employés. Plusieurs autres sont aussi dérivés des quatre cadres de référence présentés dans cette revue.

- Le *Cybersecurity framework v2.0* du National Institute of Standards and Technology (NIST) (NIST, 2024) ;
- Le *Control objectives for information and related technologies (COBIT) framework for information technology management and governance* de l'Information Systems Audit and Control Association (ISACA) (ISACA, 2018b).

Les sections suivantes présentent chacun de ces cadres[20].

5.3.1 L'*Enterprise risk management framework* du COSO

L'*Enterprise risk management framework* du COSO adresse spécifiquement les risques d'entreprise sous l'angle des impacts sur les affaires (COSO, 2004). La figure 5.1 illustre ce cadre.

Figure 5.1 L'*Enterprise risk management framework* du COSO (COSO, 2017)

Le cadre est composé de cinq composantes : (1) la gouvernance et la culture (*Governance & culture*), (2) la stratégie et les objectifs (*Strategy & objective-setting*), (3) la performance (*Performance*), (4) l'examen et la révision (*Review and revision*) et (5) l'information, les communications et la reddition (*Information, communication & reporting*). Le tableau 5.1 décrit chacune des composantes du cadre.

[20] Afin de rapporter le plus fidèlement possible le fonctionnement de ces cadres, tout le contenu qui est tiré directement des cadres est présenté dans leur langue originale (donc, en anglais). Le contenu adapté des cadres est présenté en français.

Tableau 5.1 Les cinq composantes de l'*Enterprise risk management framework* (COSO, 2017)

Composante	**Description**
Governance & culture	Governance and culture together form a basis for all other components of enterprise risk management. Governance sets the entity's tone, reinforcing the importance of enterprise risk management, and establishing oversight responsibilities for it. Culture is reflected in decision-making.
Strategy & objective-setting	Enterprise risk management is integrated into the entity's strategic plan through the process of setting strategy and business objectives. With an understanding of business context, the organization can gain insight into internal and external factors and their effect on risk. An organization sets its risk appetite in conjunction with strategy-setting. The business objectives allow strategy to be put into practice and shape the entity's day-to-day operations and priorities.
Performance	An organization identifies and assesses risks that may affect an entity's ability to achieve its strategy and business objectives. As part of that pursuit, the organization identifies and assesses risks that may affect the achievement of that strategy and business objectives. It prioritizes risks according to their severity and considering the entity's risk appetite. The organization then selects risk responses and monitors performance for change. In this way, it develops a portfolio view of the amount of risk the entity has assumed in the pursuit of its strategy and entity-level business objectives.
Review & revision	By reviewing enterprise risk management capabilities and practices, and the entity's performance relative to its targets, an organization can consider how well the enterprise risk management capabilities and practices have increased value over time and will continue to drive value in light of substantial changes.
Information, communication & reporting	Communication is the continual, iterative process of obtaining information and sharing it throughout the entity. Management uses relevant information from both internal and external sources to support enterprise risk management. The organization leverages information systems to capture, process, and manage data and information. By using information that applies to all components, the organization reports on risk, culture, and performance.

Chacune des composantes du cadre est décomposée en un certain nombre de principes. Au total, ce sont 20 principes qui sous-tendent le cadre du COSO. La figure 5.2 présente ces principes.

Figure 5.2 Les 20 principes de l'*Enterprise risk management framework* (COSO, 2017).

Chacun de ces principes est décrit par un énoncé qui en formule l'objectif et est décomposé en un certain nombre de lignes directrices qui expriment ce que, selon le cadre, devrait être la situation

dans l'organisation. Par exemple, le tableau 5.2 illustre la décomposition des deux premiers principes de la composante *Governance & culture*.

Tableau 5.2 Décomposition des principes 1 et 2 de l'*Enterprise risk management framework* (COSO, 2017)

Principe	**Énoncé du principe**	**Ligne directrice**	**Énoncé de la ligne directrice**
Exercices board risk oversight	The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.	Accountability and Responsibility	The board of directors has the primary responsibility for risk oversight in the entity.
		Skills, Experience, and Business Knowledge	The board of directors is well positioned to offer expertise and provide oversight of enterprise risk management through its collective skills, experience and business knowledge.
		Independence	The board overall should be independent. Independence enhances directors' ability to be objective and to evaluate the performance and well-being of the entity without any conflict of interest or undue influence of interested parties.
		Suitability of Enterprise Risk Management	The board engages in conversations with management to determine whether enterprise risk management is suitably designed to enhance value.
		Organizational Bias	The board is expected to understand the potential organizational biases that exist and challenge management to overcome them.
Establishes Operating Structures	The organization establishes operating structures in the pursuit of strategy and business objectives. The operating structure is typically aligned with the legal structure and management structure.	Operating Structure and Reporting Lines	The organization establishes an operating structure and designs reporting lines to carry out the strategy and business objectives.
		Enterprise Risk Management Structures	Management plans, organizes, and carries out the entity's strategy and business objectives in accordance with the entity's mission, vision, and core values.
		Authority and Responsibilities	The board delegates to management the authority to design and implement practices that support the achievement of strategy and business objectives.
			Management defines roles and responsibilities for the overall entity and its operating units. Management also defines roles, responsibilities, and accountabilities of individuals, teams, divisions, and functions aligned to strategy and business objectives.
		Enterprise Risk Management within the Evolving Entity	Enterprise risk management should be tailored to the capabilities of the entity, considering both what the organization is seeking to attain and the way it manages risk. Management, therefore, regularly evaluates the operating structure and associated reporting lines.

Sur le plan des risques, les principes 6 à 20 forment un processus qui est très similaire à celui préconisé par la norme ISO31000. Ainsi, le tout débute avec le besoin pour l'organisation de définir

le contexte d'affaires dans lequel elle opère (Principe 6 – *Analyzes business contex*t). À cette étape, l'organisation doit identifier sa mission, sa vision et ses valeurs ainsi que les environnements interne et externe dans lesquels elle opère. Les paramètres de caractérisation de ces environnements sont présentés au tableau 5.3.

Tableau 5.3 Caractérisation des environnements interne et externe de l'organisation selon le COSO (COSO, 2017)

Environnement	**Catégorie**	**Description**
External	Political	Nature and extent of government intervention and influence, including tax policies, labor laws, environmental laws, trade restrictions, tariffs, and political stability.
	Economic	Interest rates, inflation, foreign exchange rates, availability of credit, GDP growth, etc.
	Social	Customer needs or expectations; population demographics, such as age distribution, educational levels, distribution of wealth.
	Technological	R&D activity, automation, and technology incentives; rate of technological changes or disruption.
	Legal	Laws (e.g., employment, consumer, health and safety), regulations, and/or industry standards.
Internal	Capital	Assets, including cash, equipment, property, patents.
	People	Knowledge, skills, attitudes, relationships, values, and culture.
	Process	Activities, tasks, policies, or procedures.
	Technology	New, amended, and/or adopted technology.

Ensuite, l'organisation doit déterminer son profil de risque, son appétit pour le risque et sa capacité maximale de prise de risque (c'est-à-dire le niveau maximal de risque qu'elle est prête à prendre) (Principe 7 – *Defines risk appetite*). Le résultat de cette analyse devrait être représenté sous la forme d'un graphique qui représente le risque en fonction de la performance comme celui illustré à la figure 5.3[21].

[21] Le cadre ne mentionne pas comment calculer les différentes valeurs de risque qui apparaissent dans le graphique. Cela dit, le cadre mentionne à la section 3.2 : « Organizations may develop different approaches for conceptualizing and depicting the entity's risk profile » (COSO, 2017, p.15) ce qui suggère qu'il s'agit simplement d'une représentation conceptuelle.

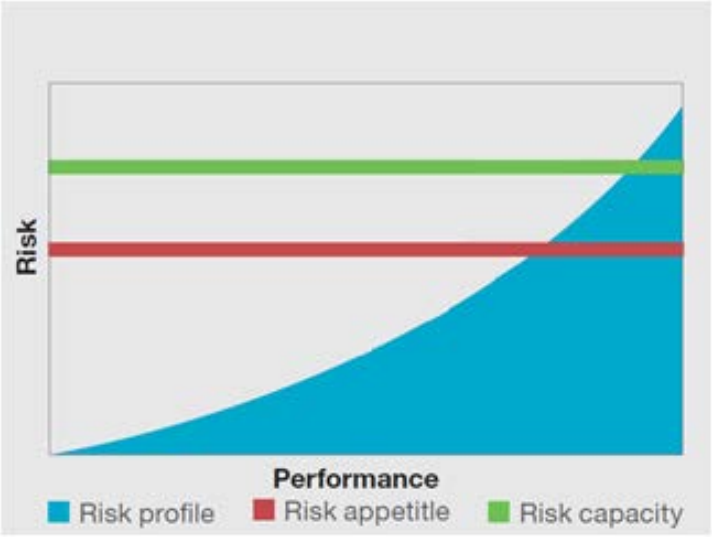


Figure 5.3 Différents repères de risques selon le COSO (COSO, 2017)

Ensuite, l'organisation doit définir ses objectifs d'affaires. Pour chacun de ces objectifs, elle doit indiquer sa cible ainsi que les mesures de performance de ces objectifs. Le résultat d'une telle analyse est contenu dans un tableau comme celui présenté au tableau 5.4.

Tableau 5.4 Objectifs d'affaires, mesures de performance et cibles selon le COSO (COSO, 2017)

Business objective		**Performance measure and target**
Business objective (entity)	• Continue to develop innovative products that interest and excite consumers. • Expand retail presence in the health food sector.	• 8 products in R&D at all times. • 5% growth year over year.
Business objectives for Confectionary (operating unit)	• Develop high-quality and safe snack products that exceed consumer expectations.	• 4.8 out of 5 in customer satisfaction survey.
Business objectives for Human Resources (function)	• Maintain favorable annual turnover of employees. • Recruit and train product sales managers in the coming year.	• Turnover less than 10%. • Recruit 50 sales managers. • 95% training rate for sales staff.

Ensuite, pour chaque objectif d'affaires, l'organisation doit indiquer son seuil de tolérance (*Tolerance*) par rapport à cette cible. Le résultat d'une telle analyse devrait être représenté sous la forme d'un graphique comme celui illustré à la figure 5.4, qui illustre la cible et la tolérance de l'objectif d'affaires « A ».

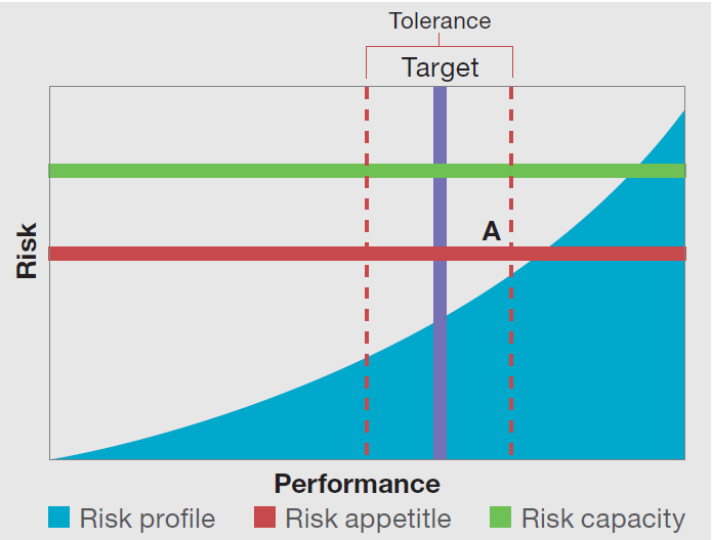


Figure 5.4 Cible et tolérance pour un objectif d'affaires donné selon le COSO (COSO, 2017)

Ensuite, toujours pour chaque objectif d'affaires, une analyse de risques doit être réalisée. Le tableau 5.5 présente un exemple d'une telle analyse de risque pour deux objectifs d'affaires.

Tableau 5.5 Analyse de risques pour deux objectifs d'affaires selon le COSO (COSO, 2017)

Objective type	**Business objective**	**Target and tolerance**	**Identified risk**	**Severity measures**	
				Rating/ Impact type	**Likelihood/ Probability**
Business objectives for snacks	Continue to develop innovative products that interest and excite consumers.	**Target:** 8 products in development at all times. **Tolerance:** Number of new products in development to be between 6 and 12 at all times.	The possibility that the organization fails to develop new products that exceed customer expectations.	Moderate impact to consumer satisfaction.	Possible
Business objectives for human resources	Recruit and train product sales managers in the coming year.	**Target:** Recruit 50 product sales managers. **Tolerance:** The entity recruits between 35 and 50 product managers in the coming year.	The possibility that the organization is unable to identify appropriately qualified people for sales managers.	Minor impact to operational/ human resources.	Possible

Ainsi, dans cet exemple, on remarque que deux objectifs d'affaires ont été listés et les cibles et les tolérances pour ces deux objectifs d'affaires ont été identifiées. Ensuite, un risque a été identifié pour chacun de ces objectifs d'affaires et une valeur d'impact et une valeur de probabilité ont été

données à ce risque. Les risques ainsi déterminés sont ensuite répertoriés dans une matrice de risques comme celle illustrée à la figure 5.5.

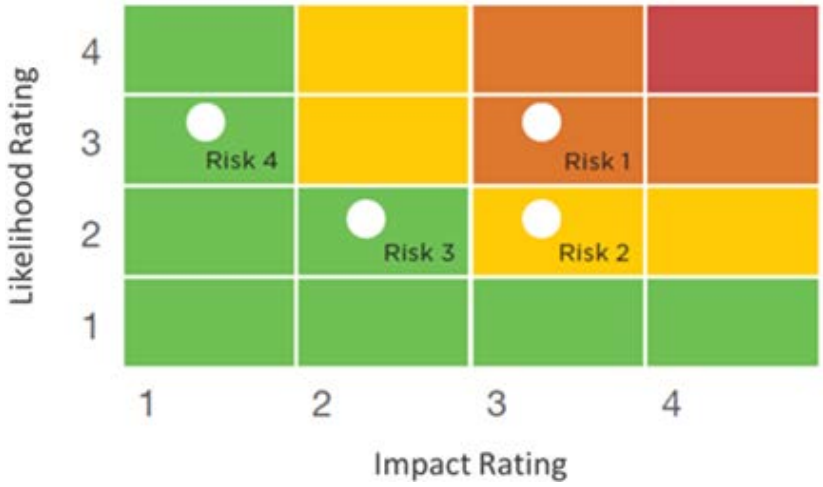


Figure 5.5 Matrice de risques proposée par le COSO (COSO, 2017)

Au niveau du suivi des risques, la performance réelle liée à l'objectif d'affaires doit faire l'objet d'un suivi périodique afin de déterminer où elle se situe par rapport à la cible. Lorsque la performance réelle se situe à l'extérieur de la zone de tolérance, des mesures doivent être prises afin de ramener la performance dans sa zone d'acceptabilité. Le résultat d'une telle analyse est présenté à la figure 5.6.

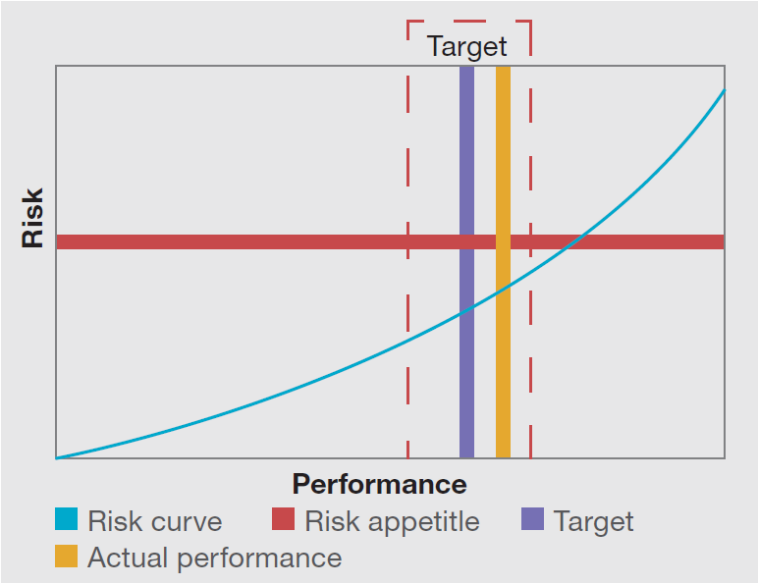


Figure 5.6 Performance réelle vs cible selon le COSO (COSO, 2017)

Finalement, les principes 18 à 20 concernent la composante *Information, communication & reporting* du cadre. Alors que le principe 18 est plus général et suggère aux organisations de tirer profit des systèmes d'information, le principe 19 présente des lignes directrices concernant les mécanismes (ou canaux de communications) que l'organisation devrait mettre en place pour assurer une communication efficace avec le conseil d'administration et les actionnaires. Finalement, le principe 20 concerne la manière dont la reddition devrait se faire. Les tableaux 5.6 et 5.7 présentent respectivement la décomposition des principes 19 et 20 selon leurs lignes directrices.

Tableau 5.6 Décomposition du principe 19 de l'*Enterprise risk management framework* (COSO, 2017)

Principe	**Énoncé du principe**	**Ligne directrice**	**Énoncé de la ligne directrice**
Principle 19 Communicates Risk Information	The organization uses communication channels to support enterprise risk management.	Communicating with Stakeholders	Management communicates the entity's strategy and business objectives clearly throughout the organization so that all personnel at all levels understand their individual roles.
			Management communicates information about the entity's strategy and business objectives to shareholders and other external parties. Enterprise risk management is a key topic in these communications.
		Communicating with the Board	Organizations should examine their governance structure to ensure that responsibilities are clearly allocated and defined at the board and management levels and that the structure supports the desired risk dialogue.
			The board of directors and management must have a shared understanding of risk and its relationship to strategy and business objectives.
		Methods of Communicating	To be sure communication methods are working, organizations should periodically evaluate them. This can be done through existing processes such as stating expectations for enterprise risk management in employee performance goals and subsequent periodic performance evaluations.
			Separate lines of communication are needed when normal channels are inoperative or insufficient for communicating matters requiring heightened attention. Many organizations provide a means to communicate anonymously to the board of directors or a board delegate - such as a whistle-blower hotline. Many organizations also establish escalation protocols and policies to facilitate communication when there are exceptions in standards of conduct or inappropriate behaviors occurring.

Tableau 5.7 Décomposition du principe 20 de l'*Enterprise risk management framework* (COSO, 2017)

Principe	**Énoncé du principe**	**Ligne directrice**	**Énoncé de la ligne directrice**
Principle 20 Reports on Risk, Culture, and Performance	The organization reports on risk, culture, and performance at multiple levels and across the entity.	Identifying Report Users and Their Roles	Risk reporting may be done by any team within the operating structure. Teams prepare reports, disclosing information in accordance with their risk management responsibilities.
		Reporting Attributes	Reporting combines quantitative and qualitative risk information. Risk information supports management in decision-making, although management must still exercise judgment in the pursuit of business objectives as well as the business context.
		Types of Reporting	Risk reporting is supplemented by commentary and analysis by subject matter experts.
		Reporting Risk to the Board	There are a number of ways management may report to a board, but it is critical that the focus of reporting be the link between strategy, business objectives, risk, and performance.
		Reporting on Culture	Reporting on culture may be embodied in: • Analytics of cultural trends. • Benchmarking to other entities or standards. • Compensation schemes and the potential influence on decision-making. • Lessons learned analyses. • Reviews of behavioural trends. • Surveys of risk attitudes and risk awareness.
		Key Indicators	Key indicators are reported along with corresponding targets and acceptable variations.
		Reporting Frequency and Quality	Management works closely with those who will use reports to identify what information is required, how often they need the reports, and their preferences in how reports are presented. Management is responsible for implementing appropriate controls so that reporting is accurate, clear, and complete.

Ainsi, le cadre du COSO est organisé principalement en deux grands volets : (1) un volet associé à la dimension gouvernance des risques et (2) un volet associé à la dimension technique des risques.

Sur le plan de la gouvernance, le cadre positionne la gestion des risques d'entreprise comme étant presque exclusivement l'affaire du conseil d'administration et de la haute direction. Ainsi, plusieurs des lignes directrices concernent spécifiquement ces deux groupes. Cependant, ces lignes

directrices mentionnent globalement ce qui devrait être fait (dans le cas idéal) et qui devrait le faire, mais sans mentionner comment le faire.

Sur le plan technique, le cadre est beaucoup plus prescriptif et propose le processus à suivre afin d'identifier, analyser et évaluer les risques, sous l'angle des impacts sur les affaires. À cet effet, le processus est très similaire à celui proposé par la norme ISO31000, mais les graphiques permettant de comparer les performances réelles et cibles par rapport aux différents seuils de risques sont spécifiques à ce cadre. Cependant, comparativement à la norme ISO31000, une différence majeure dans la manière dont le cadre adresse les risques existe. En effet, comme le cadre du COSO est centré sur la mission de l'organisation, le risque n'est pas associé à un aléa externe ou interne qui pourrait affecter la réalisation d'un objectif d'affaires et auquel on associe une probabilité d'occurrence. Il est plutôt associé à la non-atteinte d'un objectif d'affaires lui-même. Ainsi, lorsqu'on considère l'objectif stratégique d'affaires 1 (lié à la production de collations) (tableau 5.5), celui-ci comprend un objectif d'affaires qui est de « continuer à produire des collations innovantes et intéressantes pour les clients » et le risque associé à cet objectif d'affaires est de « ne pas être en mesure de produire des collations innovantes et intéressantes pour les clients ». Ensuite, la probabilité est associée au risque lui-même et l'impact est associé, on suppose, à la mission de l'organisation ou à un objectif d'affaires plus stratégique qui comprendrait plusieurs objectifs dont celui pour lequel l'analyse de risques est faite[22].

5.3.2 Le *Risk governance framework* de l'IRGC

Le *Risk governance framework* de l'IRGC (IRGC, 2017) est un autre cadre largement reconnu dans le domaine de la gestion des risques. Dans ce cadre, la gestion des risques est scindée en deux grands volets : (1) la compréhension des risques (associée à la génération et l'évaluation des connaissances sur les risques) et (2) la prise de décisions en regard de la gestion des risques.

[22] Cette approche de calcul du risque est différente de celle voulant que le risque soit le résultat de la probabilité d'occurrence d'un aléa quelconque (interne ou externe à l'organisation) par la somme de ses conséquences. Dans cet exemple, il semble que le COSO suggère d'évaluer comment la non-atteinte d'un objectif d'affaires impacte l'objectif d'affaires stratégique auquel il est lié ou la mission de l'organisation. Ensuite, une probabilité (ou possibilité/plausibilité (*likelihood*)) est associée à ce « scénario ». Cette manière de fonctionner s'apparente davantage à l'approche par conséquences développée par le CRP. Celle-ci ne s'intéresse pas aux causes (aléas) ayant conduit à une défaillance, mais évalue plutôt les effets d'une défaillance sur le fonctionnement de l'organisation et sa capacité à remplir sa mission (c'est-à-dire, fournir sa propre ressource). Ensuite, une analyse permet de déterminer si les mesures de mitigation et contrôle sont bien en place pour éviter une telle situation ou en réduire les conséquences. Par contre, dans l'approche par conséquences, on ne s'intéresse pas à associer une probabilité au « scénario » de défaillance lui-même.

Ce cadre s'articule autour de cinq grandes composantes : (1) l'analyse préliminaire (*Pre-assessment*), (2) l'évaluation (*Appraisal*), (3) la caractérisation et l'évaluation (*Characterisation and evaluation*), (4) la gestion (*Management*) et (5) l'aspect transversal de la gestion des risques (*Cross-cutting aspects*) (en lien avec la communication et de l'engagement des parties prenantes). La figure 5.7 présente ce cadre.

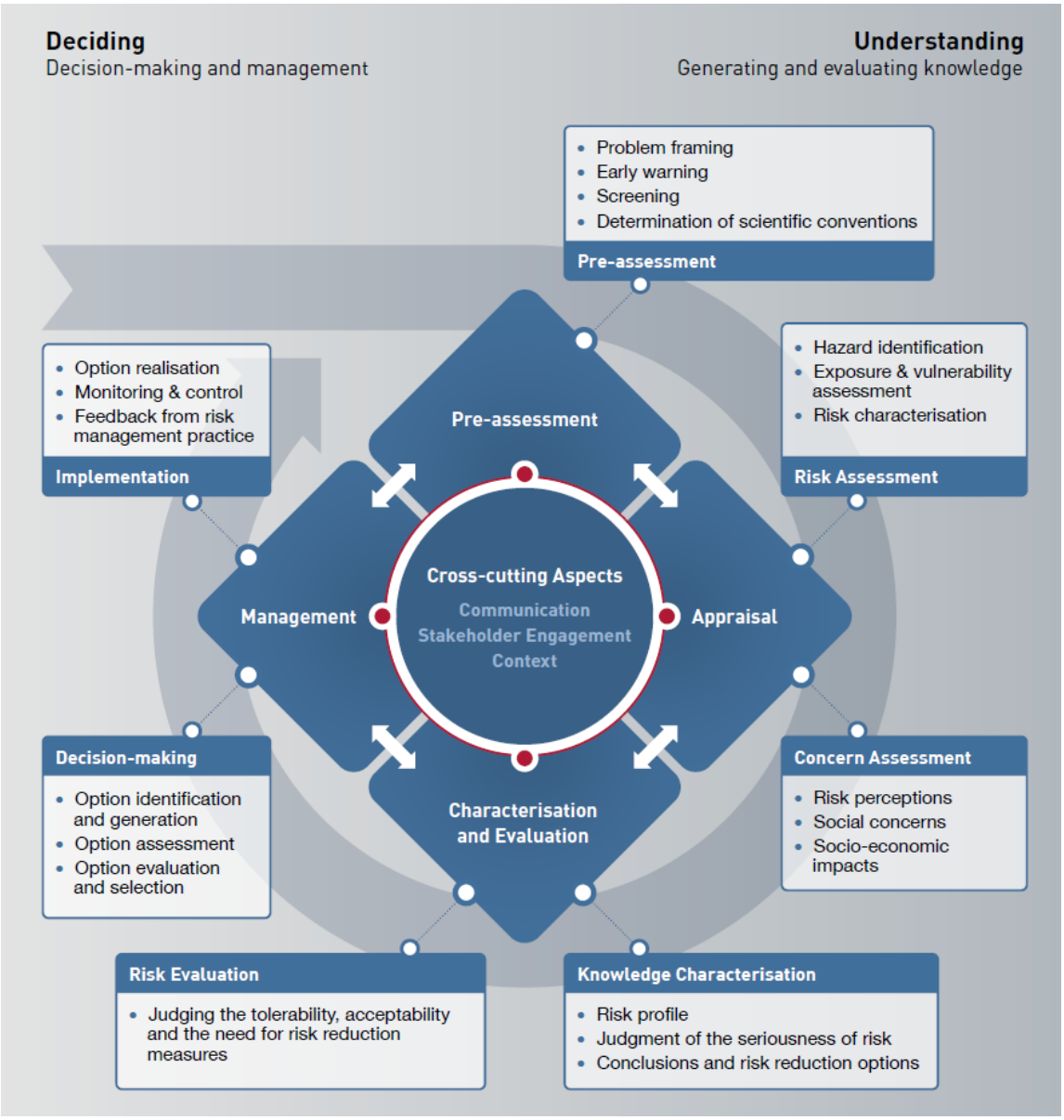


Figure 5.7 Le *Risk governance framework* de l'IRGC (IRGC, 2017)

Si les quatre premières composantes s'enchaînent comme un processus, la cinquième composante s'applique à toutes les autres composantes. Le tableau 5.8 présente les énoncés qui décrivent chacune de ces composantes.

Tableau 5.8 Les cinq composantes du *Risk governance framework* (IRGC, 2017)

Composante	**Énoncé**
Pre-assessment	Identification and framing; setting the boundaries of the risk or system.
Appraisal	Assessing the technical and perceived causes and consequences of the risk.
Characterisation and evaluation	Making a judgment about the risk (its acceptability) and the need to manage it.
Management	Deciding on and implementing risk management options.
Cross-cutting aspects	Communicating, engaging with stakeholders, considering the context.

Le *Risk governance framework* de l'IRGC présente des caractéristiques très similaires à la norme ISO31000 et suit foncièrement les mêmes grandes étapes. Les sections suivantes (adaptées du cadre) expliquent chacune de ces étapes.

Étape 1 : Analyse préliminaire (*Pre-assessment*)

L'analyse préliminaire est la première étape du processus proposé dans le cadre de l'IRGC. Cette étape vise à saisir les différentes perspectives du risque, les opportunités associées et les stratégies potentielles pour y remédier. Selon l'IRGC, l'analyse préliminaire devrait permettre de répondre à des questions comme :

- Quels sont les risques et les opportunités?
- Qui sont les parties prenantes ?
- Comment leurs opinions affectent-elles la définition et formulation du problème ?
- Quels sont les enjeux organisationnels ?
- Quelles sont les différentes dimensions du risque ?
- Quelles sont les limites, en termes de portée, d'échelle ou d'horizon temporel ?
- Existe-t-il des indications qu'il y a déjà un problème ? Est-il nécessaire d'agir ?
- Quels sont les outils et les méthodes qui peuvent être utilisés pour évaluer les risques ? De nouveaux protocoles de recherche doivent-ils être mis en place pour caractériser les risques ?
- Quels sont les systèmes juridiques/réglementaires en place et comment affectent-ils le problème ?
- L'analyse prospective est-elle employée afin d'identifier les risques émergents ?
- Quelle est la capacité des gouvernements, des organisations et des personnes impliquées à prendre en charge ces risques ?

Étape 2 : Analyse des risques (*Risk assessment*)

L'analyse des risques est la deuxième étape du processus proposé dans le cadre de l'IRGC. L'analyse a pour objectif de développer (voire, renforcer) la connaissance nécessaire à la prise de décision relative au risque, à savoir s'il doit être géré ou non, et si oui, quelles options sont envisageables. Pour cela, l'IRGC propose d'identifier les possibilités d'occurrence de conséquences négatives résultant de l'exposition des biens (ou valeurs) à des aléas auxquels ils sont vulnérables. L'analyse de risque devrait permettre de répondre à des questions comme :

- Quels sont les dommages potentiels ou les effets indésirables associés au risque?
- Ces dommages ou effets sont-ils irréversibles ?
- Quels scénarios d'accident peuvent survenir ?
- Qu'en est-il de leur gravité, de leur dynamique, de leur probabilité d'occurrence, etc. ?
- Le risque peut-il être quantifié ?
- Les estimations des probabilités sont-elles fiables ?
- Quel est le niveau d'incertitude ?
- Quel est le niveau de confiance dans l'évaluation des risques ?
- Les facteurs pertinents ont-ils tous été pris en compte ?
- Les données ayant servi aux analyses sont-elles fiables ?

Étape 3 : Analyse des préoccupations (*Concern assessment*)

L'analyse des préoccupations est la troisième étape du processus proposé dans le cadre de l'IRGC. Il s'agit de recueillir les opinions des différentes parties prenantes et leurs inquiétudes et à en faire une analyse systématique. Cette phase est spécifique au processus de l'IRGC en ce sens qu'elle n'apparaît pas directement dans les processus de gestion des risques traditionnels (ISO31000). Pour l'IRGC, il s'agit, à cette étape, de reconnaître que les décisions des individus en regard des risques sont influencées par leurs expériences passées, leur perception des risques ainsi que par des préoccupations émotionnelles ou leurs valeurs personnelles. Afin d'intégrer ces variables dans l'analyse des risques, l'IRGC recommande de mettre en place un processus collaboratif visant à permettre aux individus de développer leur intelligence situationnelle et d'accroître leur compréhension des risques, surtout dans des contextes plus complexes ou incertains. L'analyse des préoccupations devrait permettre de répondre à des questions comme :

- Quelles sont les opinions, les valeurs et les préoccupations des différentes parties prenantes au sujet du risque ?
- Existe-t-il des biais cognitifs qui affectent la perception du risque ?
- Existe-t-il des contraintes sociologiques, organisationnelles et anthropologiques chez les acteurs et les parties prenantes ?
- Quel rôle jouent les institutions existantes, les structures de gouvernance et les médias dans la définition et la prise en compte des préoccupations du public ?
- Les gestionnaires de risques sont-ils susceptibles de faire face à des controverses et des conflits en raison de différences dans la perception du risque, dans les objectifs et les valeurs des parties prenantes, ou en raison de possibles inégalités dans la répartition des avantages et des inconvénients liés aux risques ?

Étape 4 : Caractérisation des connaissances

La caractérisation des connaissances est la quatrième étape du processus proposé dans le cadre de l'IRGC. À cette étape, il s'agit de caractériser les connaissances sur les risques afin de déterminer, pour chaque risque, de quel type de risque il s'agit. Le tableau 5.9 illustre les types de risques et les connaissances qui les caractérisent.

Tableau 5.9 Type de risques et caractérisation des connaissances (IRGC, 2017)

Type de risque	**Caractérisation des connaissances**
Simple	Les risques simples sont caractérisés par des causes et des conséquences relativement connues et ne sont pas sujet de controverses.
Complexe	Les risques complexes sont caractérisés par des difficultés à identifier et quantifier précisément les causes et les conséquences. Les connaissances sur ces risques doivent provenir de recherches scientifiques ou empiriques et de travaux spécialisés.
Incertain	Les risques incertains sont caractérisés par un manque de données scientifiques ou techniques ou un manque de clarté ou de qualité de ces données. La confiance en ces connaissances est faible.
Ambigu	Les risques ambigus sont caractérisés par des points de vue divergents sur tous les paramètres du risque, y compris la probabilité et la gravité des effets indésirables potentiels. Ces risques font plus facilement l'objet de polémiques et de conflits et soulèvent des questions éthiques qui dépendent des valeurs et des intérêts des personnes.

Étape 5 : Évaluation des risques

L'évaluation des risques est la cinquième étape du processus proposé dans le cadre de l'IRGC. À cette étape, il s'agit de poser un jugement sur l'acceptabilité des risques. Pour cela, l'IRGC propose

trois statuts pour un risque : 1) acceptable, (2) tolérable et (3) intolérable. Les risques acceptables ne doivent faire l'objet d'aucune mesure particulière ; les risques tolérables doivent faire l'objet de mesures de réduction des risques ; les risques intolérables doivent être évités le plus possible. Si aucune mesure d'évitement ou de substitution ne peut être mise en place, alors des mesures de réduction des risques doivent être adoptées afin de rendre ces risques tolérables. La figure 5.8 illustre la matrice de risque telle que présentée dans le cadre IRGC.

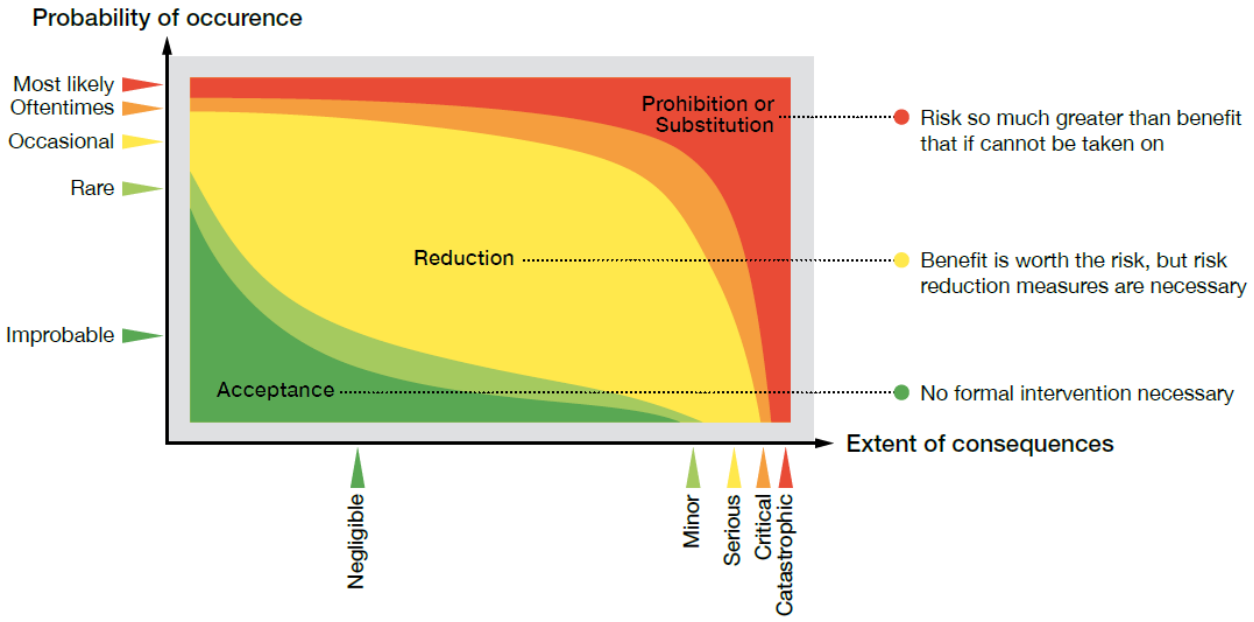


Figure 5.8 Matrice d'évaluation des risques proposée par l'IRGC (IRGC, 2017)

Lors de l'évaluation des risques, l'IRGC recommande de tenir compte des facteurs suivants :

- Y a-t-il des questions éthiques à prendre en considération, au-delà de celles prises en compte dans l'évaluation des préoccupations ?
- Quelles sont les valeurs et les normes sociétales pour porter des jugements sur la tolérabilité et l'acceptabilité ?
- Y a-t-il des parties prenantes – gouvernements, entreprises ou autres – qui ont des engagements ou d'autres raisons de vouloir un résultat particulier du processus de gouvernance des risques ?
- Quelles sont les contraintes (par exemple, temps, budget, contexte, etc.) ?

- Quelle est l'appréciation politique ou stratégique des avantages et des risques sociétaux, économiques et environnementaux ?
- Y a-t-il une possibilité de substitution ? Si oui, comment les risques se comparent-ils ?

Étape 6 : Prise de décisions

La prise de décision est la sixième étape du processus proposé dans le cadre de l'IRGC. Celle-ci réfère à l'identification des mesures de mitigation des risques à mettre en place. À cet effet, l'IRGC propose quatre différentes stratégies de gestion des risques selon le type de risque. Ces stratégies sont présentées au tableau 5.10.

Tableau 5.10 Stratégies de gestion recommandées par l'IRGC en fonction du type de risque (IRGC, 2017)

Type de risque	**Stratégie de gestion**
Simple	Les risques simples peuvent être gérés à l'aide d'une stratégie opérationnelle ou par l'adoption d'une loi ou d'un règlement.
Complexe	Les risques complexes doivent être gérés en fonction des recommandations formulées par des experts et s'appuyant sur des modèles scientifiques.
Incertain	Les risques incertains doivent être gérés à l'aide de stratégies fondées sur le principe de précaution et axées sur la résilience des systèmes et la réduction de leurs vulnérabilités.
Ambigu	Les risques ambigus doivent être gérés à l'aide de stratégies fondées sur la discussion et la compréhension mutuelle et impliquant l'ensemble des parties prenantes concernées.

Étape 7 : Mise en oeuvre

La mise en oeuvre est la dernière étape du processus proposé dans le cadre de l'IRGC. Simplement, elle revient à implémenter les mesures de mitigation des risques identifiées à l'étape 6.

Aspects transversaux (Communication, engagement des parties prenantes et contexte)

La communication et l'engagement des parties prenantes ne constituent pas une étape du processus puisqu'elle s'applique à chaque étape, exactement comme le prévoit aussi la phase de « Communication et consultation » prévue dans la norme ISO31000. Ainsi, le cadre de l'IRGC recommande d'impliquer tous les acteurs, les groupes d'intérêts et les parties prenantes concernés à chaque étape du processus. Selon la complexité des risques, les parties prenantes varient. La figure 5.9 illustre les parties prenantes à impliquer dans le processus en fonction du type de risque.

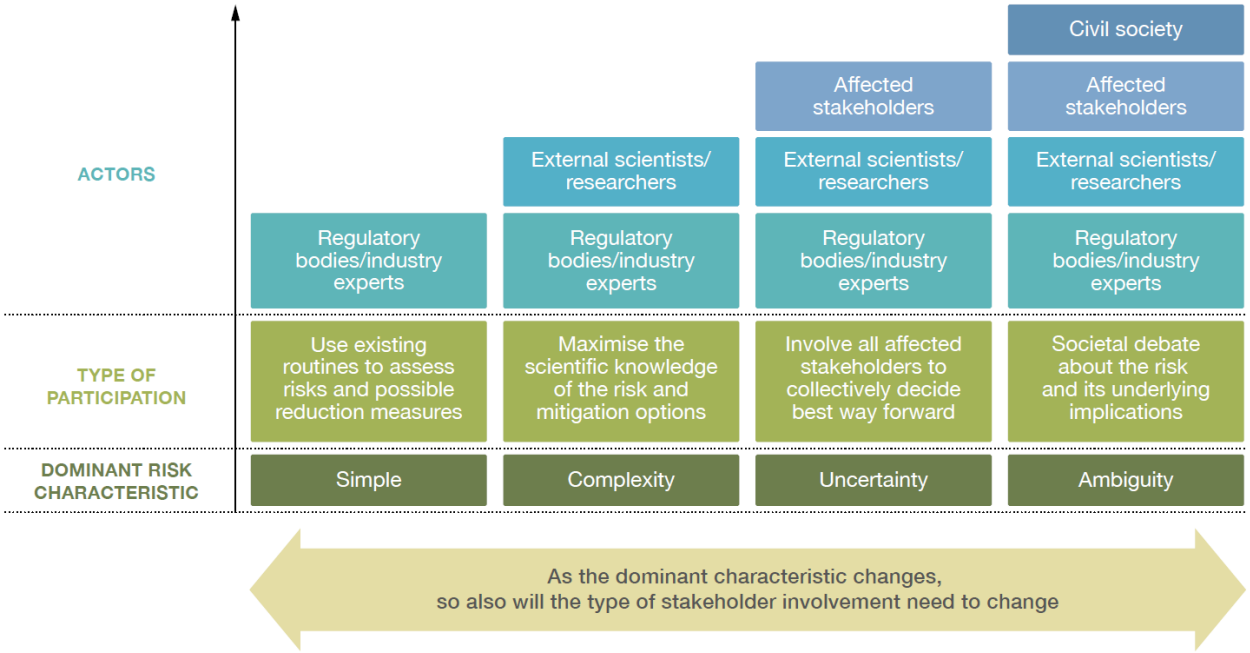


Figure 5.9 Parties prenantes à impliquer selon le type de risque selon l'IRGC (IRGC, 2017)

Au-delà du processus, l'IRGC formule aussi certaines mises en garde qu'il qualifie de « déficits de gouvernance potentiels ». Le tableau 5.11 présente ces mises en garde pour chaque étape du processus.

Tableau 5.11 Les déficits de gouvernance potentiels selon l'IRGC (IRGC, 2017)

Étape du processus	**Déficits de gouvernance potentiels**
Pre-assessment	• Warning – Signals of a known risk have not been detected or recognised (complacency bias, false positive and false negative). • Scope – A risk which is perceived as having only local consequences may in fact be much broader (and vice-versa). • Framing – Different stakeholders may have conflicting views on the issue (including contesting views about the desirability of the benefits). • 'Black swans' (surprising extreme events relative to our knowledge) – No awareness of a hazard or possible risk.
Risk assessment	• Lack of appropriate methods and models to assess potential harm (e.g. in the case of new technologies or cumulative exposure). • Scarcity of scientific data about the risk (risk agent and risk-absorbing system) and/or about stakeholders' associated concerns. • Inappropriate use of advanced assessment methods, such as those deriving from big data analytics, artificial intelligence, social media analysis, or citizen science.
Concern assessment	• Misunderstanding about biases that may affect the perception of the risk. • Low confidence level in the data, the model or their interpretation. • Inadequate attention given to the concerns of different stakeholder groups, and drivers of their behaviour.

Étape du processus	**Déficits de gouvernance potentiels**
Knowledge characterization	*Le cadre ne fait mention d'aucun déficit de gouvernance à cette étape du processus.*
Risk evaluation	• Overlooking outcomes from risk appraisal – Failing to fully consider social needs, environmental impacts, cost-benefit analyses and risk-benefit balances. • Exclusion – When some stakeholders and their views or significant benefits and other consequences are excluded or omitted, whether advertently or inadvertently. • Indecision – When there is lack of responsiveness, due to a voluntary act of authority or an involuntary failure in the decision-making process (e.g. overly inclusive process with stakeholders may lead to inertia). • Lack of transparency and accountability – When trade-offs are not made explicit and resolved, and hidden agendas (including of experts involved) may determine the outcome of the evaluation process. • Sustainability – When risk decision is not robust and relevant for a long period
Decision-making	• Lack of responsibility – No entity is legally responsible for failures; risk management and regulation may 'fall between the cracks'. • Lack of accountability – Decision-makers are isolated from the impact of their decision. • Unsustainability – E.g. short-term decisions lead to further longer-term problems. • Short-term expediency – Authority makes a decision on a knee-jerk or ad-hoc basis, for instance as a response to public pressure. • Indecision/lack of timeliness – Delays or inaction make matters worse. • Inequity – Decisions allot the risk and benefits unfairly.
Implementation	• Failing implementation – Decisions are ignored or poorly implemented. • Lack of evaluation and feedback – Implementation is poorly evaluated, feedback is not integrated into review. • Inappropriate use of advanced management tools, such as those deriving from artificial intelligence and machine-learning. • Inflexibility – Failure to revisit a risk decision in the light of new knowledge.
Cross-cutting aspects	• One-way information instead of two-way communication prevents building a dialogue. • Communication from experts is often too technical to be understood by lay people and stakeholders. Such communication may not address what stakeholders need and want to know. It may not account for how different stakeholders receive and accept information. • Communication is not adapted to the category of risk (simple, complex, uncertain, ambiguous). For example, it does not convey uncertainty. • People's or organisations' concerns are treated as irrelevant or irrational; this may cause incomplete understanding of the full nature of risks as well as social mobilisation against the institution or the final decision. • Low level of confidence or trust in the decision-making process, the information given or the communication channel weakens the whole process. • Exclusion – Accidental or deliberate exclusion of stakeholders and/or their views. • 'Authority knows best' – A deliberate refusal to communicate with other interested parties leads the stakeholders with power to make the decisions, irrespective of the need for consultation and dialogue. • Ignoring the composition of complexity, uncertainty and ambiguity and designing a process that is either too inclusive (for rather trivial risks) or not inclusive enough (for ambiguous risks). • Insufficient attention to changes in context and to stakeholders' nature and expectations. • 'Paralysis by analysis' – Selection of an overly inclusive process leads to inertia or indecision. • Time pressure and time delay – The deliberative process is under time constraint or is diluted.

Ainsi, le cadre de l'IRGC est scindé en deux grands volets : (1) la compréhension des risques et (2) la prise de décisions en regard de la gestion des risques. Il est structuré globalement de la même manière que la norme ISO31000.

Sur le plan de la gouvernance, le cadre n'aborde que très peu (voire, presque pas) la question des rôles et des responsabilités des différentes parties prenantes. Plutôt, un noyau central concernant les aspects transversaux à prendre en compte à chaque étape du processus a été ajouté afin de s'assurer que la dimension gouvernance des risques soit présente dans le cadre, mais sans plus. Cependant, exactement comme la phase de communication et consultation que l'on retrouve dans la norme ISO31000, ce noyau central se limite à mentionner que la communication et l'engagement des parties prenantes sont nécessaires à toutes les étapes du processus, mais avec un ajout supplémentaire intéressant concernant l'identification des déficits de gouvernance possibles à chaque étape du processus. Ces considérations ont pour objectif de susciter la réflexion au niveau des personnes appliquant le cadre afin de s'assurer qu'elles ont bien considéré tous les aspects transversaux dans leurs analyses et qu'ils ont intégré l'ensemble des parties prenantes dans le processus, mais aussi afin de les mettre en garde contre certains aspects qui pourraient impacter négativement le processus, comme les perceptions individuelles, les intérêts divergents, la balance des avantages et des inconvénients liés aux risques, etc. En somme, il semble que ce cadre soit davantage orienté vers la gestion des risques qui concernent plus globalement la population, par exemple, les risques associés aux grands projets d'infrastructures.

Sur le plan technique, il s'agit essentiellement du même processus de gestion des risques que la norme ISO31000, mais auquel certaines étapes supplémentaires comme l'analyse des préoccupations (étape 3) et la caractérisation des connaissances (étape 4) ont été ajoutées. La catégorisation des risques en quatre différents types (simple, complexe, incertain ou ambigu) est aussi intéressante et spécifique à ce cadre.

5.3.3 Le *Cybersecurity framework v2.0* du NIST

Le *Cybersecurity framework v2.0* du NIST (NIST, 2024) est un autre cadre de référence largement reconnu dans le domaine de la gestion des risques. Ce cadre est orienté vers la gestion des risques cybernétiques. Néanmoins, les concepts peuvent aisément être généralisés à tous les risques[23].

Selon le NIST (2024), le cadre de référence a été établi afin de fournir des conseils aux organisations pour réduire les risques de cybersécurité. Le cadre a été conçu pour être utilisé par des organisations de toutes tailles et de tous secteurs. Contrairement aux cadres précédents, qui sont découpés selon des processus de gestion des risques plus conventionnels, le cadre du NIST suit un découpage qui s'apparente davantage aux quatre dimensions de la sécurité civile (prévention, préparation, intervention, rétablissement) (Gouvernement du Québec, 2008a).

Le cadre du NIST comprend six fonctions : (1) la gouvernance (*Govern*), (2) l'identification (*Identify*), (3) la protection (*Protect*), (4) la détection (*Detect*), (5) la réponse (*Respond*) et (6) le rétablissement (*Recover*). Comme c'est le cas dans le cadre de l'IRGC, les cinq fonctions en périphérie du cadre forment un processus, alors que la fonction « gouvernance » s'applique à toutes les fonctions. La figure 5.10 présente le cadre proposé par le NIST.

Figure 5.10 Le *Cybersecurity framework v2.0* (NIST, 2024)

[23] Le NIST possède aussi un autre cadre plus général pour la gestion des risques. Il s'agit du *Risk management framework for information systems and organizations* (NIST, 2018b). Cependant, ce cadre se veut une forme « généralisée » dérivée du *Cybersecurity framework*. Ainsi, le premier réfère pratiquement toujours au second, si bien que pour les besoins de cette thèse, c'est ce dernier cadre qui est analysé.

Le tableau 5.12 présente les six fonctions du cadre NIST.

Tableau 5.12 Les six fonctions du cadre NIST (NIST, 2024)

Fonction	**Énoncé**	**Description**
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.
Identify	The organization's current cybersecurity risks are understood.	Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.
Protect	Safeguards to manage the organization's cybersecurity risks are used.	Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
Respond	Actions regarding a detected cybersecurity incident are taken.	RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
Recover	Assets and operations affected by a cybersecurity incident are restored.	RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

Chacune des fonctions du cadre NIST est divisée en un certain nombre de catégories. Au total, 22 catégories sont associées aux fonctions du cadre NIST. Celles-ci sont présentées au tableau 5.13.

Tableau 5.13 Catégories associées aux fonctions du cadre NIST (NIST, 2024)

Fonctions	Catégories	Identifiants
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity supply chain management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RS.RP
	Incident Recovery Communication	RC.CO

Chacune de ces catégories est divisée en un certain nombre de sous-catégories dont chacune est énoncée sous la forme d'une ligne directrice qui comporte un ou plusieurs éléments à valider. Par exemple, la catégorie *Organizational context* (GV.OC) est divisée en 4 sous-catégories alors que la catégorie *Risk management strategy* (GV.RM) est divisée en 7 sous-catégories. Au total, ce sont 106 sous-catégories qui sont identifiées dans le cadre NIST. Le tableau 5.14 montre la décomposition des catégories GV.OC et GV.RM en leurs sous-catégories respectives.

Tableau 5.14 Décomposition des catégories GV.OC et GV.RM du cadre NIST (NIST, 2024)

GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood. • **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management. • **GV.OC-02:** Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered. • **GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed. • **GV.OC-04:** Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated. • **GV.OC-05:** Outcomes, capabilities, and services that the organization depends on are understood and communicated.
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions. • **GV.RM-01:** Risk management objectives are established and agreed to by organizational stakeholders. • **GV.RM-02:** Risk appetite and risk tolerance statements are established, communicated, and maintained. • **GV.RM-03:** Cybersecurity risk management activities and outcomes are included in enterprise risk management processes. • **GV.RM-04:** Strategic direction that describes appropriate risk response options is established and communicated. • **GV.RM-05:** Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties. • **GV.RM-06:** A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated. • **GV.RM-07:** Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions.

Pour chacune de ces sous-catégories, le cadre NIST prévoit que l'organisation évalue à quel niveau de maturité elle se situe. Quatre niveaux sont proposés par le NIST et leur description est adaptée selon la catégorie faisant l'objet de l'évaluation. Ces niveaux s'appliquent donc autant aux catégories liées à la gouvernance qu'à celles liées à la gestion des risques. Ces niveaux sont décrits au tableau 5.15.

Tableau 5.15 Niveaux de maturité proposés par le NIST (NIST, 2024)

Tier	Risk Governance	Risk Management
Tier 1 Partial	Application of the organizational cybersecurity risk strategy is managed in an ad hoc manner.	• There is limited awareness of cybersecurity risks at the organizational level. • The organization implements cybersecurity risk management on an irregular, case-by-case basis.

Tier	Risk Governance	Risk Management
	Prioritization is ad hoc and not formally based on objectives or threat environment.	• The organization may not have processes that enable cybersecurity information to be shared within the organization. • The organization is generally unaware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses.
Tier 2 Informed	Risk management practices are approved by management but may not be established as organization-wide policy. The prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	• There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. • Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring. • Cybersecurity information is shared within the organization on an informal basis. • The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks.
Tier 3 Repeatable	The organization's risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape.	• There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization. • Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. • The organization consistently and accurately monitors the cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Executives ensure that cybersecurity is considered through all lines of operation in the organization. • The organization risk strategy is informed by the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. These actions are implemented consistently and as intended and are continuously monitored and reviewed.
Tier 4 Adaptive	There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.	• The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced

Tier	Risk Governance	Risk Management
	The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture. It evolves from an awareness of previous activities and continuous awareness of activities on organizational systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.	cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats. • The organization uses real-time or near real-time information to understand and consistently act upon the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. • Cybersecurity information is constantly shared throughout the organization and with authorized third parties.

Sur le plan de la gouvernance, le cadre vise à évaluer si l'organisation a bien identifié sa mission (GV.OC-01) et ses objectifs (GV.OC-04), ses politiques et ses processus (GV.PO) et si les rôles et les responsabilités ont bien été assignés à toutes les parties prenantes (GV.RR). Sur le plan technique, le cadre vise à évaluer si l'organisation a bien identifié un seuil d'acceptabilité des risques (GV.RM-02) et si elle a adopté un modèle standardisé pour catégoriser, calculer et prioriser les risques (GV.RM-06). Ainsi, le cadre du NIST ne fait que formuler des objectifs (sous-catégories) pour chacune des catégories du cadre. Ce faisant, il n'est aucunement prescriptif, ni sur le plan de la dimension gouvernance des risques ni sur le plan de la dimension technique des risques. Il ne mentionne donc absolument pas comment faire les choses, comment atteindre chacun des objectifs ou comment les mettre en pratique.

Tout compte fait, le cadre NIST s'apparente davantage à un modèle permettant d'évaluer la maturité de l'organisation en lien avec la gestion des risques cybernétiques. Une organisation qui souhaiterait adopter ce cadre pourrait aisément en élargir la portée pour considérer les autres risques (donc, dans le cadre d'une approche de GIR). En répondant par oui ou non aux multiples sous-catégories, l'organisation peut évaluer sa maturité et identifier les éléments sur lesquels elle doit travailler pour l'améliorer.

5.3.4 Le *COBIT framework for information technology management and governance* de l'ISACA

Le *COBIT framework for information technology management and governance* de l'ISACA (ISACA, 2018a) adresse la gouvernance et la gestion des technologies de l'information dans les organisations. Comme le cadre NIST, il ne s'agit donc pas spécifiquement d'une cadre pour la gestion des risques, encore moins pour la GIR. Néanmoins, il contient tout un volet sur les risques, ce qui explique qu'il soit utilisé aussi dans le contexte de la gestion des risques.

Le cadre COBIT est relativement rigide en ce sens que tout a déjà été défini dans le cadre. Probablement, parce que le cadre COBIT a été pensé pour pouvoir être informatisé en tant qu'outil de gestion des technologies de l'information. La figure 5.11 illustre l'écosystème COBIT 2019.

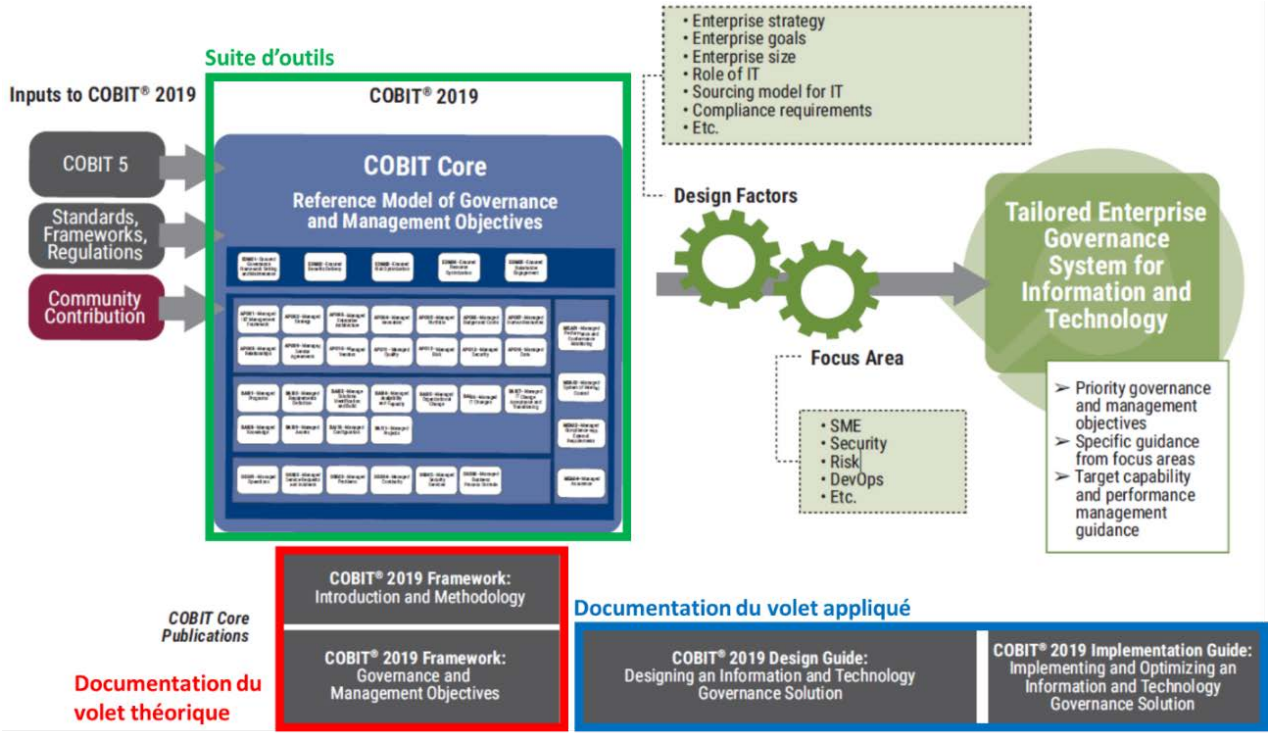


Figure 5.11 Le *COBIT framework for information technology management and governance* (ISACA, 2018a)

Dans l'encadré vert (COBIT Core), ce sont les outils ; dans l'encadré bleu, ce sont les documents associés au volet appliqué du cadre ; dans l'encadré rouge, ce sont les documents associés au volet

théorique du cadre. Dans le cadre de cette revue, seulement les éléments qui traitent du volet théorique du cadre seront analysés[24].

Le cadre COBIT s'articule autour de 40 objectifs de gouvernance et de gestion catégorisés dans les cinq domaines suivants :

1. Évaluer, diriger et encadrer (*Evaluate, Direct and Monitor* – EDM) ;
2. Aligner, planifier et organiser (*Align, Plan and Organize* – APO) ;
3. Construire, acquérir et implémenter (*Build, Acquire and Implement* – BAI) ;
4. Livrer, maintenir et supporter (*Deliver, Service and Support* – DSS) ;
5. Suivre, analyser et évaluer (*Monitor, Evaluate and Assess* – MEA).

Les objectifs liés à la gouvernance se retrouvent dans le domaine EDM qui contient cinq objectifs. Les quatre autres domaines (APO, BAI, DSS et MEA) sont les domaines de gestion. Ceux-ci contiennent 35 objectifs.

La figure 5.12 présente les 40 objectifs du cadre COBIT. Dans l'encadré rouge, ce sont les cinq objectifs du domaine de la gouvernance, alors que dans l'encadré vert ce sont les 35 objectifs des domaines de la gestion. Dans le domaine de la gouvernance, l'objectif EDM03 – *Ensured risk optimization* (encadré orange) est d'un plus grand intérêt pour cette revue ; dans les domaines de gestion, c'est l'objectif APO12 – *Managed risk* (encadré jaune).

[24] Le cadre COBIT 2019 s'articule autour de quatre documents supportant la suite COBIT. Ces documents sont les suivants : COBIT® 2019 Framework: Introduction and Methodology, COBIT® 2019 Framework: Governance and Management Objectives, COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution, COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution. Dans le cadre de cette revue, seuls les deux premiers ont été analysés (les deux derniers documents sont les pendants opérationnels des concepts présentés dans les deux premiers documents).

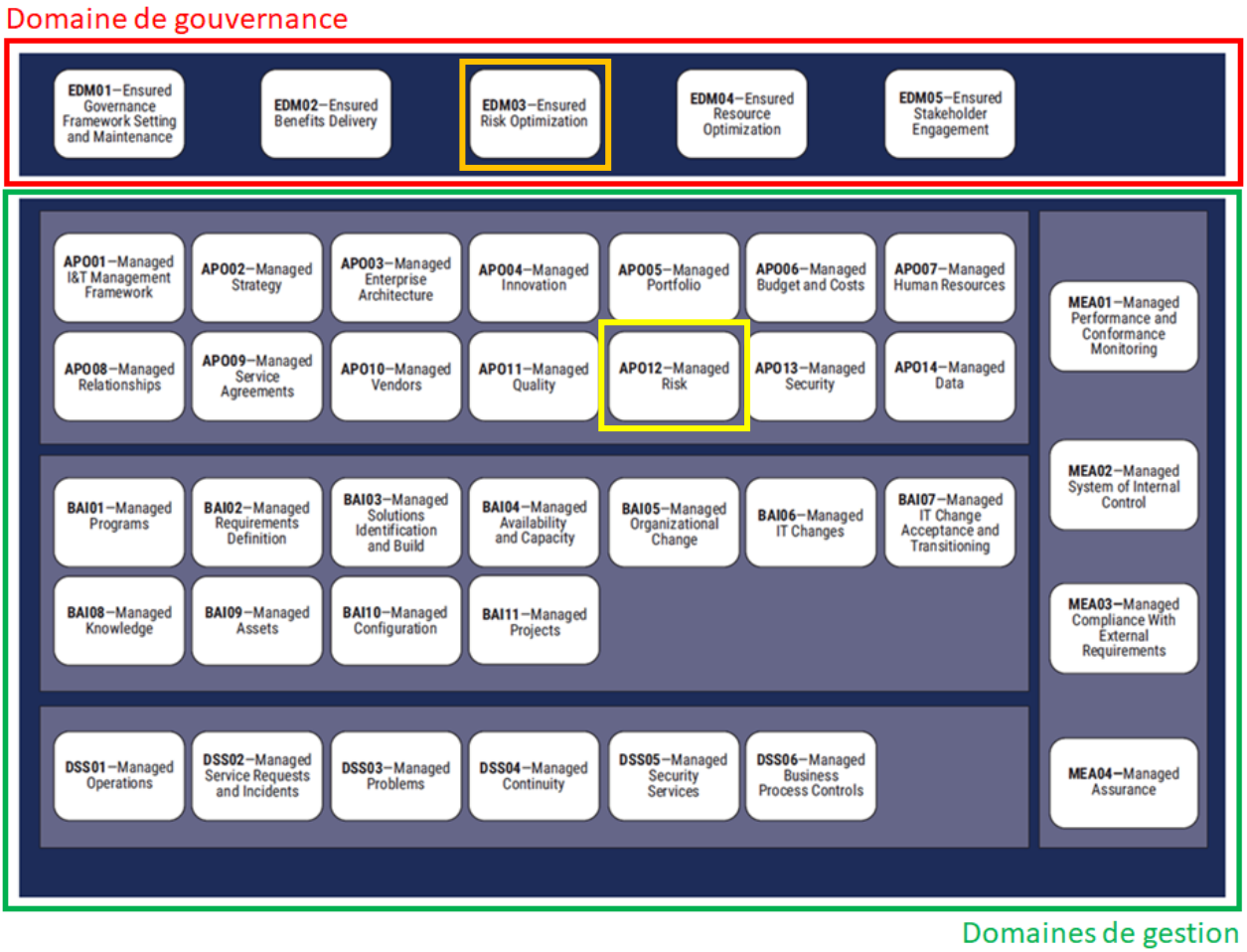


Figure 5.12 Les 40 objectifs du cadre COBIT (ISACA, 2018a)

Chacun des 40 objectifs du cadre COBIT est détaillé dans une fiche qui décrit l'objectif lui-même, la raison d'être de l'objectif, les métriques associées à l'objectif ainsi que les objectifs liés. Ces derniers sont répertoriés en deux catégories : (1) les objectifs d'entreprise (*Enterprise Goals* (EG)) et (2) les objectifs d'alignement (*Alignment Goals* (AG)). Dans le cadre, ces objectifs sont déjà tous répertoriés et codés selon un numéro séquentiel. Au total, 40 fiches sont donc disponibles dans COBIT. Le tableau 5.16 présente l'une de ces fiches. Celle-ci est associée au troisième objectif du domaine EDM, soit l'objectif EDM03 – *Ensured risk optimization*.

Tableau 5.16 Fiche relative à l'objectif EDM03 – *Ensured risk optimization* (ISACA, 2018b)

Domain: Evaluate, Direct and Monitor Governance Objective: EDM03 – Ensured Risk Optimization	Focus Area: COBIT Core Model
Description	
Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed.	
Purpose	
Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.	
The governance objective supports the achievement of a set of primary enterprise and alignment goals:	
Enterprise Goals	**Alignment Goals**
• EG02 Managed business risk • EG06 Business service continuity and availability	• AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals	**Example Metrics for Alignment Goals**
EG02 a. Percent of critical business objectives and services covered by risk assessment b. Ratio of significant incidents that were not identified in risk assessments vs. total incidents c. Frequency of updating risk profile	AG02 a. Frequency of updating risk profile b. Percent of enterprise risk assessments including I&T-related risk c. Number of significant I&T-related incidents that were not identified in a risk assessment
EG06 a. Number of customer service or business process interruptions causing significant incidents b. Business cost of incidents c. Number of business processing hours lost due to unplanned service interruptions d. Percent of complaints as a function of committed service availability targets	AG07 a. Number of confidentiality incidents causing financial loss, business disruption or public embarrassment b. Number of availability incidents causing financial loss, business disruption or public embarrassment c. Number of integrity incidents causing financial loss, business disruption or public embarrassment

Le tableau 5.17 présente quant à lui les objectifs d'entreprise (EG) et les objectifs d'alignement (AG) définis dans le cadre.

Tableau 5.17 Objectifs d'entreprise et objectifs d'alignement selon COBIT 2019 (ISACA, 2018b)

Objectifs d'entreprise (*EG*)		**Objectifs d'alignement (*AG*)**	
Code	**Description**	**Code**	**Description**
EG01	Portfolio of competitive products and services	AG01	I&T compliance and support for business compliance with external laws and regulations
EG02	Managed business risk	AG02	Managed I&T-related risk
EG03	Compliance with external laws and regulations	AG03	Realized benefits from I&T-enabled investments and services portfolio
EG04	Quality of financial information	AG04	Quality of technology-related financial information
EG05	Customer-oriented service culture	AG05	Delivery of I&T services in line with business requirements
EG06	Business service continuity and availability	AG06	Agility to turn business requirements into operational solutions
EG07	Quality of management information	AG07	Security of information, processing infrastructure and applications, and privacy

Objectifs d'entreprise (*EG*)		Objectifs d'alignement (*AG*)	
EG08	Optimization of business process functionality	AG08	Enabling and supporting business processes by integrating applications and technology
EG09	Optimization of business process costs	AG09	Delivering programs on time, on budget and meeting requirements and quality standards
EG10	Staff skills, motivation and productivity	AG10	Quality of I&T management information
EG11	Compliance with internal policies	AG11	I&T compliance with internal policies
EG12	Managed digital transformation programs	AG12	Competent and motivated staff with mutual understanding of technology and business
EG13	Product and business innovation	AG13	Knowledge, expertise and initiatives for business innovation

Le domaine de la gouvernance est formé de sept composantes : (1) les processus (*Processes*), (2) les structures organisationnelles (*Organizational structures*), (3) les principes, les politiques et les procédures (*Principles, policies, procedures*), (4) l'information (*Information*), (5) la culture, l'éthique et les comportements (*Culture, ethics and behavior*), (6) les personnes, les habiletés et les compétences (*People, skills and competencies*) et (7) les services, les infrastructures et les applications (*Services, infrastructure and applications*). Ces composantes du domaine de la gouvernance sont illustrées à la figure 5.13.

Figure 5.13 Les sept composantes de la gouvernance selon COBIT 2019 (ISACA, 2018a)

Pour chacun des objectifs du domaine de la gouvernance (donc, du domaine EDM), le cadre prévoit que chacune des composantes de la gouvernance soit détaillée. Ainsi, comme ce domaine contient cinq objectifs et que sept composantes sont associées à la gouvernance, ce sont 35 fiches en tout qui concernent ce domaine. Le tableau 5.18 illustre un exemple d'une telle fiche.

Tableau 5.18 Fiche relative au processus EDM03.01 – Evaluate risk management (ISACA, 2018b)

A. Component: Process	
Governance Practice	**Example Metrics**
EDM03.01 Evaluate risk management. Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	a. Level of unexpected enterprise impact b. Percent of I&T risk that exceeds enterprise risk tolerance c. Refreshment rate of risk factor evaluation

Activities	Capability Level
1. Understand the organization and its context related to I&T risk.	2
2. Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.	
3. Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.	
4. Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.	
5. Proactively evaluate I&T risk factors in advance of pending strategic enterprise decisions and ensure that risk considerations are part of the strategic enterprise decision process.	3
6. Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.	
7. Attract and maintain necessary skills and personnel for I&T Risk Management	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16

Cette fiche représente le premier des trois processus liés à l'objectif EDM03 – *Ensured risk optimization*, soit le processus EDM03.01 – *Evaluate risk management*. Ce processus comprend sept activités (que l'on pourrait associer à des lignes directrices). Pour chaque processus, le cadre fournit des références supplémentaires aux organisations qui désirent adopter le cadre. Dans ce cas-ci, on remarque que le cadre COBIT réfère au cadre du COSO 2017 (voir encadré jaune dans le tableau 5.18). Ensuite, pour chacune des activités identifiées, l'organisation doit s'évaluer en s'attribuant une note de 0 à 5 correspondant au niveau de maturité auquel elle estime se situer (voir encadré rouge dans le tableau 5.18). Pour cela, le cadre COBIT utilise l'échelle du Capability Maturity Model Integration (CMMI) adapté aux processus. La figure 5.14 illustre et décrit ces différents niveaux.

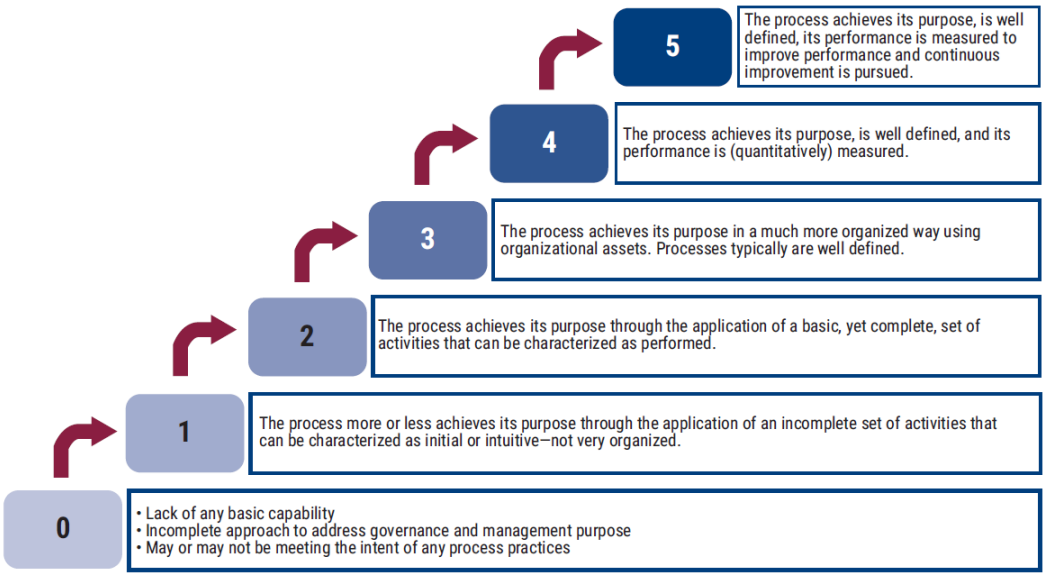


Figure 5.14 Les six niveaux de maturité des processus considérés par COBIT (ISACA, 2018a)

La deuxième composante de la gouvernance est les structures organisationnelles. Le tableau 5.19 illustre la fiche liée à la structure organisationnelle de l'objectif EDM03 – *Ensured risk optimization*. Cette fiche présente les trois processus liés à l'atteinte de cet objectif ainsi que les acteurs qui en sont responsables (sous la forme d'une matrice de type RACI (*Responsible, Accountable, Consulted, Informed*)).

Tableau 5.19 Fiche relative à la composante « structures organisationnelles » de l'objectif EDM03 (ISACA, 2018b)

B. Component: Organizational Structures								
Key Governance Practice	Board	Executive Committee	Chief Executive Officer	Chief Risk Officer	Chief Information Officer	I&T Governance Board	Enterprise Risk Committee	Chief Information Security Officer
EDM03.01 Evaluate risk management.	A	R	R	R	R	R	R	
EDM03.02 Direct risk management.	A	R	R	R	R	R	R	
EDM03.03 Monitor risk management.	A	R	R	R	R	R	R	R

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance

Concernant les acteurs, le cadre COBIT 2019 prédéfinit 33 rôles différents. Ceux-ci sont présentés au tableau 5.20.

Tableau 5.20 Les 33 rôles (acteurs) prédéfinis dans COBIT 2019 (ISACA, 2018b)

Rôles prédéfinis dans COBIT 2019		
Architecture Board	Chief Risk Officer	I&T Governance Board
Audit	Chief Technology Officer	Information Security Manager
Board	Compliance	Legal Counsel
Business Continuity Manager	Data Management Function	Portfolio Manager
Business Process Owner	Enterprise Risk Committee	Privacy Officer
Chief Digital Officer	Executive Committee	Program Manager
Chief Executive Officer	Head Architect	Project Management Office
Chief Financial Officer	Head Development	Project Manager
Chief Information Officer	Head Human Resources	Relationship Manager
Chief Information Security Officer	Head IT Administration	Service Manager
Chief Operating Officer	Head IT Operations	Steering (Programs/Projects) Committee

La composante « flux d'information » présente comment les informations voyagent à travers la suite COBIT. Le tableau 5.21 présente le flux d'information des trois processus liés à l'objectif EDM03 – *Ensured risk optimization*.

Tableau 5.21 Fiche relative à la composante « flux d'information » de l'objectif EDM03 (ISACA, 2018b)

C. Component: Information Flows and Items (see also Section 3.6)				
Governance Practice	**Inputs**		**Outputs**	
EDM03.01 Evaluate risk management.	**From**	**Description**	**Description**	**To**
	APO12.01	Emerging risk issues and factors	Risk appetite guidance	APO04.01; APO12.03
	Outside COBIT	Enterprise risk management (ERM) principles	Evaluation of risk management activities	APO12.01
			Approved risk tolerance levels	APO12.03
EDM03.02 Direct risk management.	APO12.03	Aggregated risk profile, including status of risk management actions	Approved process for measuring risk management	APO12.01
	Outside COBIT	Enterprise risk management (ERM) profiles and mitigation plans	Key objectives to be monitored for risk management	APO12.01
			Risk management policies	APO12.01
EDM03.03 Monitor risk management.	APO12.02	Risk analysis results	Remedial actions to address risk management deviations	APO12.06
	APO12.04	• Risk analysis and risk profile reports for stakeholders • Results of third-party risk assessments • Opportunities for acceptance of greater risk	Risk management issues for the board	EDM05.01
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.5 Assessment (Tasks 1, 2): Inputs 2, and Outputs; 3.6 Authorization (Task 1): Inputs and Outputs			

Concernant les composantes « principes, politiques et procédures », « culture, éthique et comportements », « personnes, habiletés et compétences » et « services, infrastructures et applications », dans la très grande majorité des fiches, le cadre ne fait que fournir des références à d'autres documents qui adressent spécifiquement ces items. Les tableaux 5.22 à 5.25 présentent les fiches associées à ces composantes.

Tableau 5.22 Fiche relative à la composante « politiques et procédures » de l'objectif EDM03 (ISACA, 2018b)

E. Component: Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Enterprise risk policy	Defines governance and management of enterprise risk at strategic, tactical and operational levels, pursuant to business objectives. Translates enterprise governance into risk governance principles and policy and elaborates risk management activities.	National Institute of Standards and Technology Special Publication 800- 53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-1)

Tableau 5.23 Fiche relative à la composante « culture, éthique et comportement » de l'objectif EDM03 (ISACA, 2018b)

F. Component: Culture, Ethics and Behavior		
Key Culture Elements	**Related Guidance**	**Detailed Reference**
Promote an I&T risk-aware culture at all levels of the organization and empower the enterprise proactively to identify, report and escalate I&T risk, opportunity and potential business impacts. Senior management sets direction and demonstrates visible and genuine support for risk practices. Additionally, management must clearly define risk appetite and ensure an appropriate level of debate as part of business-as-usual activities. Desirable behaviors include encouraging employees to raise issues or negative outcomes and show transparency with regard to I&T risk. Business owners should accept ownership of I&T risk when applicable and demonstrate genuine commitment to I&T risk management by providing adequate resource levels.	COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principles 3 and 4

Tableau 5.24 Fiche relative à la composante « personne, habiletés et compétences » de l'objectif EDM03 (ISACA, 2018b)

D. Component: People, Skills and Competencies		
Skill	**Related Guidance (Standards, Frameworks, Compliance Requirements)**	**Detailed Reference**
Business risk management	Skills Framework for the Information Age V6, 2015	BURM
Risk management	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

Tableau 5.25 Fiche relative à la composante « services, infrastructure et applications » de l'objectif EDM03 (ISACA, 2018b)

G. Component: Services, Infrastructure and Applications
• COBIT and related products/tools • Equivalent frameworks and standards

Concernant la dimension technique du risque, le cadre COBIT fait référence, entre autres, aux cadres du COSO et du NIST et aux normes sur la sécurité de l'information ISO27001:2013 et ISO27005:2011. Le cadre COBIT fournit donc une série d'activités liées à l'évaluation des risques qui sont un condensé des principales lignes directrices de ces différents cadres/normes. Celles-ci sont principalement réparties entre les processus EDM03.01 – *Evaluate risk management* sous l'objectif de gouvernance EDM03 – *Ensured risk optimization* et les processus APO12.02 –

Analyze risk et APO12.06 – *Respond to risk* sous l'objectif de gestion APO12 – *Managed risk*. Les tableaux 5.26 à 5.28 illustrent ces processus et montrent que l'approche préconisée par le cadre COBIT est donc, elle aussi, similaire à celle préconisée par la norme ISO31000. Dans ces tableaux, les activités similaires à ces normes ont été encadrées en jaune ; les références qui ont été utilisées afin d'établir ces activités sont encadrées en rouge.

Tableau 5.26 Processus EDM03.01 – *Evaluate risk management* du cadre COBIT (ISACA, 2018b)

A. Component: Process	
Governance Practice	**Example Metrics**
EDM03.01 Evaluate risk management. Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	a. Level of unexpected enterprise impact b. Percent of I&T risk that exceeds enterprise risk tolerance c. Refreshment rate of risk factor evaluation

Activities	Capability Level
1. Understand the organization and its context related to I&T risk.	2
2. Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.	
3. Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.	
4. Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.	
5. Proactively evaluate I&T risk factors in advance of pending strategic enterprise decisions and ensure that risk considerations are part of the strategic enterprise decision process.	3
6. Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.	
7. Attract and maintain necessary skills and personnel for I&T Risk Management	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16

Tableau 5.27 Processus APO12.02 – *Analyze risk* du cadre COBIT (ISACA, 2018b)

A. Component: Process	
Management Practice	**Example Metrics**
APO12.02 Analyze risk. Develop a substantiated view on actual I&T risk, in support of risk decisions.	a. Number of identified I&T risk scenarios b. Time since last update of I&T risk scenarios

Activities	Capability Level
1. Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.	3
2. Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.	
3. Estimate the frequency (or likelihood) and magnitude of loss or gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.	
4. Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.	
5. Propose risk responses for risk exceeding risk appetite and tolerance levels.	
6. Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.	
7. Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.	4
8. Analyze cost/benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 11
ISF, The Standard of Good Practice for Information Security 2016	IR2.1 Risk Assessment Scope; IR2.2 Business Impact Assessment
ISO/IEC 27001:2013/Cor.2:2015(E)	8.2 Information security risk assessment
ISO/IEC 27005:2011(E)	8.3 Risk analysis
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.RA Risk Assessment
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 3)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-3)

Tableau 5.28 Processus APO12.06 – *Respond to risk* du cadre COBIT (ISACA, 2018b)

A. Component: Process	
Management Practice	**Example Metrics**
APO12.06 Respond to risk. Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	a. Number of measures not reducing residual risk b. Percent of I&T risk action plans executed as designed

Activities	Capability Level
1. Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.	3
2. Apply the appropriate response plan to minimize the impact when risk incidents occur.	
3. Categorize incidents and compare I&T-related loss exposures against risk tolerance thresholds. Communicate business impacts to decision makers as part of reporting and update the risk profile.	4
4. Examine past adverse events/losses and missed opportunities and determine root causes.	
5. Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers. Ensure that the cause, response requirements and process improvement are included in risk governance processes.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 13
ISF, The Standard of Good Practice for Information Security 2016	IR2.9 Risk Treatment
ISO/IEC 27001:2013/Cor.2:2015(E)	6.1 Action to address risk and opportunities
ISO/IEC 27005:2011(E)	9. Information security risk treatment
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 4)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-9, PM-31)

Ainsi, le cadre COBIT est construit de manière similaire aux cadres du COSO et du NIST. Sur le plan de la gouvernance et sur le plan technique, ces trois cadres sont donc très similaires. Toutefois, le cadre COBIT est beaucoup plus détaillé et rigide que les deux autres. Au niveau du détail, le cadre COBIT est pratiquement un condensé de lignes directrices provenant de plusieurs cadres et de normes de référence. Comme les autres cadres analysés, il mentionne donc ce qui devrait être fait, mais il ne mentionne pas comment le faire. Au niveau de la rigidité, tout a déjà été défini dans le cadre, jusqu'aux activités associées aux différents processus, aux acteurs qui ont un rôle à jouer dans ces processus et aux compétences que devraient avoir ces acteurs. De plus, les flux d'informations échangées entre les différents modules de la suite COBIT font en sorte que les organisations qui décideraient de mettre en place ce cadre (ou l'outil) s'y adaptent, et non l'inverse. Cela peut demander un énorme travail de redéfinition des façons de faire, de réattribution des rôles et des responsabilités et de mise en place d'une structure organisationnelle qui soit en adéquation avec la structure du cadre. Finalement, comme le cadre du NIST, celui-ci permet d'évaluer la maturité de l'organisation en lien avec la gestion des risques. En proposant d'utiliser l'échelle du CMMI et en permettant d'associer un niveau de maturité à chaque activité, l'organisation peut évaluer sa maturité globale et identifier les éléments qui doivent être améliorés.

5.4 Les politiques, les guides et les lignes directrices

Les politiques, les guides et autres lignes directrices relatives à la GIR et qui émanent de gouvernements ou autres autorités compétentes sont d'autres types de documents que l'on retrouve dans la littérature. Parmi ces documents, et sur une base davantage nationale, on retrouve le Guide de gestion intégrée du risque du Gouvernement du Canada (Gouvernement du Canada, 2016), le Modèle de politique en gestion intégrée des risques du Gouvernement du Québec (Gouvernement du Québec, 2022) et les Lignes directrices sur la gestion intégrée des risques de l'Autorité des Marchés Financiers (AMF, 2015).

5.4.1 Le Guide de gestion intégrée du risque du Gouvernement du Canada

Le Guide de gestion intégrée du risque du Gouvernement du Canada a été publié en 2016. Il s'adresse spécifiquement aux fonctionnaires fédéraux ainsi qu'aux personnes responsables de la gestion des risques dans les différents ministères et organismes relevant du Gouvernement du Canada. Comme c'est le cas pour les cadres analysés à la section précédente, les concepts sont suffisamment généraux pour pouvoir être appliqués à n'importe quelle organisation. D'ailleurs, le cadre lui-même utilise l'expression « les organisations » pour faire référence aux différents ministères et organismes liés au gouvernement.

Sur le plan de la gouvernance, le modèle s'articule autour de neuf principes. Ceux-ci sont présentés au tableau 5.29.

Tableau 5.29 Les neuf principes du cadre de GIR du Gouvernement du Canada (Gouvernement du Canada, 2016)

Principe de gouvernance	**Énoncé**
Appuyer la prise des décisions et le respect des priorités à l'échelle du gouvernement, ainsi que la réalisation des objectifs organisationnels et l'obtention des résultats prévus, tout en maintenant la confiance du public.	Ce principe vise à encourager les organisations à mettre en oeuvre la gestion du risque d'une manière appuyant le programme global du gouvernement. De façon générale, les pratiques de gestion du risque devraient permettre de relever, dans l'ensemble de l'organisation, de l'information sur les risques pouvant servir à appuyer la prise de décisions au sein du gouvernement et être assez souples pour évoluer au même rythme que les priorités gouvernementales. L'approche de gestion du risque adoptée par une organisation devrait aussi appuyer les décisions internes en permettant de relever et de gérer les risques particuliers à leurs propres objectifs et résultats attendus.
Être adaptée et réagir aux contextes externes et internes de l'organisation, y compris son mandat, ses priorités, sa culture de risques organisationnels, sa	Ce principe vise à encourager les organisations à mettre en place des mécanismes de gestion du risque adaptés à leur contexte et à leurs besoins particuliers et adaptables aux changements. Il n'existe aucune approche

Principe de gouvernance	Énoncé
capacité de gestion des risques et les intérêts de ses partenaires et intervenants.	universelle de gestion du risque, et les organisations doivent tenir compte de leur contexte propre pour définir l'approche adéquate.
Ajouter de la valeur en tant qu'élément clé du processus décisionnel, de la planification opérationnelle, de l'attribution des ressources et de la gestion des opérations.	Ce principe engage les organisations à appliquer leurs mécanismes de gestion du risque et l'information qu'ils permettent de rassembler à l'ensemble de leurs pratiques de gestion et à leur processus de prise de décisions. La gestion du risque ne doit pas être une pratique dissociée ; elle devrait plutôt être intégrée aux structures et aux processus organisationnels en place.
Assurer un équilibre entre le degré d'intervention en réponse aux risques et les contrôles établis et favoriser la souplesse et l'innovation pour améliorer le rendement et les résultats obtenus.	Ce principe appelle les organisations à adopter des stratégies adéquates de réaction aux menaces qui ne sont toutefois pas trop contraignantes et à rester ouvertes aux possibilités. Grâce à cet équilibre, l'approche de gestion du risque peut permettre d'améliorer efficacement le rendement et les résultats.
Être transparente, inclusive, intégrée et systématique.	Ce principe appelle les organisations à adopter une approche de gestion du risque : • dont l'exécution est transparente, notamment pour ce qui est des résultats des processus de gestion du risque afin qu'ils permettent d'éclairer les décisions à l'échelle de l'organisation ; • inclusive, c'est-à-dire qu'elle inclut tous les intervenants et les décideurs concernés à tous les niveaux de l'organisation dans l'approche globale de gestion du risque et dans les processus d'évaluation des risques ; • intégrée à tous les processus décisionnels et appliquée à l'échelle de l'organisation ; • systématique, c'est-à-dire dont les processus sont explicitement définis et structurés de manière à permettre la cohérence, l'efficacité et la rapidité.
Améliorer de façon continue la culture et la capacité en matière de gestion des risques au sein des organisations fédérales.	Ce principe invite les organisations à continuellement contrôler, examiner et améliorer leur approche et leurs processus de gestion du risque afin d'en assurer l'efficacité, l'efficience et la pertinence à l'appui du rendement organisationnel global. Cette démarche permet à l'approche de gestion du risque de se développer au sein de l'organisation.
Les instruments de politiques du Conseil du Trésor (CT) devraient cibler les risques associés à la réalisation des objectifs du gouvernement fédéral.	Ce principe incite le Secrétariat du Conseil du Trésor (SCT), en qualité d'organisme central, à élaborer et à renouveler ses politiques afin qu'elles incluent des mécanismes axés sur le risque. Ainsi, les politiques devraient énoncer des attentes favorisant un rendement réduisant au minimum les menaces susceptibles de peser sur les objectifs du gouvernement fédéral et permettant de tirer le maximum des occasions d'amélioration.
Ces instruments devraient être proportionnels à la probabilité que les risques identifiés se concrétisent et aux répercussions qui y sont associées.	Ce principe convie le SCT, en qualité d'organisme central, à renouveler ses politiques de manière à ce que leurs dispositions sur la surveillance et la conformité soient suffisamment souples pour refléter l'importance des risques potentiels. Les politiques permettraient ainsi des mesures de contrôles strictes dans les secteurs susceptibles d'impliquer des conséquences graves, alors que des pouvoirs souples pourraient être attribués dans les secteurs où les risques sont moins graves.
Les activités de surveillance devraient être ajustées en fonction de la capacité d'une organisation de gérer les risques, lorsque les circonstances le permettent.	Ce principe engage le SCT, en qualité d'organisme central, à adapter les activités de surveillance aux besoins particuliers des organisations de manière à tenir compte de leurs risques propres et de la capacité qu'elles ont démontrée à gérer ces risques.

Sur le plan des rôles et des responsabilités, le cadre cible principalement deux groupes : (1) le Conseil du trésor (CT) et le Secrétariat du Conseil du trésor (CST) et (2) les administrateurs généraux des différentes organisations. Le tableau 5.30 présente les rôles et les responsabilités assignés à ces deux groupes.

Tableau 5.30 Rôles et responsabilités des différents groupes selon le cadre de GIR du Gouvernement du Canada (Gouvernement du Canada, 2016)

Groupe	**Rôles et responsabilités**
Conseil du Trésor et Secrétariat du Conseil du Trésor	Le CT et le SCT ont un rôle à jouer dans le renforcement de la gestion du risque au sein des ministères et organismes fédéraux. Un élément clé du rôle du CT, et du SCT, consiste à assurer l'excellence en gestion au gouvernement par l'intermédiaire du leadership, de l'orientation, du suivi, de l'examen et de la surveillance en vertu des pouvoirs que leur confère la Loi sur la gestion des finances publiques. Le CT et le SCT ont la responsabilité de fournir aux ministères et organismes des orientations, des outils et une expertise pour favoriser la prise en compte du risque dans le cadre de la gestion. De plus, ils jouent un rôle de leadership en communiquant de l'information et en faisant la promotion de pratiques exemplaires relatives à la gestion du risque et l'adoption d'approches éclairées par l'analyse des risques. Le SCT doit surveiller et évaluer le rendement des ministères et organismes en matière de gestion du risque, entre autres, au moyen de l'examen des vérifications internes et externes. S'il est démontré que les pratiques de gestion du risque d'un ministère ou organisme fédéral sont efficaces, il se pourrait que le CT et le SCT adaptent leur surveillance à la capacité de gestion du risque de l'organisation, lorsque les circonstances le permettent. À l'inverse, une gestion du risque inefficace peut mener à des mesures de contrôle et de surveillance supplémentaires. Le SCT peut encourager les administrateurs généraux à prendre les mesures correctives nécessaires pour qu'ils puissent bien exercer leurs responsabilités concernant la surveillance de la gestion du risque dans leur organisation.
Administrateurs généraux	Les administrateurs généraux sont chargés de gérer les risques auxquels leur organisation est exposée et de mettre en oeuvre des pratiques efficaces de gestion du risque. Un des principaux rôles des administrateurs généraux est de s'assurer que les principes et les pratiques de gestion du risque sont compris et intégrés aux diverses activités de leur organisation. En outre, les administrateurs généraux sont chargés de surveiller les pratiques de gestion du risque de leur organisation, de prendre en considération les risques associés à leurs principaux partenaires à l'intérieur et à l'extérieur de la fonction publique fédérale. Ils doivent aussi faire en sorte que les questions qui influent sur les méthodes de gestion de risques entreprises par l'organisation, qu'il s'agisse de risques relevés lors d'évaluations et d'activités de surveillance interne ou externe, sont examinées et réglées. Les administrateurs généraux jouent un rôle important dans la mise en place d'un contexte favorisant l'apprentissage qui favorise le perfectionnement des compétences et des capacités dans le domaine de la gestion du risque au sein de leur organisation. Par leur leadership, ils favorisent l'instauration d'une culture organisationnelle qui soutient une prise de décisions éclairée par l'analyse des risques, facilite le dialogue sur la tolérance au risque, met l'accent sur les résultats, permet de tenir compte des possibilités et favorise l'innovation.

Sur le plan de la dimension technique du risque, le cadre n'impose pas une manière spécifique de faire. À cet effet, le cadre reconnaît que chaque organisation, selon sa taille, sa complexité, sa culture et son niveau de maturité possède ses propres façons de faire :

> « …les ministères et organismes devraient utiliser des éléments du présent guide pour concevoir une approche et un processus de gestion du risque adaptés à leurs besoins. Les éléments ne s'appliqueront pas tous à l'ensemble des méthodes et des processus, et chacun des éléments ne nécessitera pas le même niveau de détail. Ainsi, la structure des méthodes et des processus de gestion du risque sera très différente d'une organisation à l'autre » (Gouvernement du Canada, 2016, p.14).

Néanmoins, il propose une définition du risque qui est arrimée à la définition traditionnelle du concept de risque :

> « …le risque exprime la probabilité et les répercussions d'un événement susceptible de nuire à l'atteinte des objectifs de l'organisation… Pour chaque risque considéré, il faut évaluer deux choses : la probabilité ou l'éventualité que l'événement survienne et l'ampleur de ses répercussions ou de ses conséquences s'il survient » (Gouvernement du Canada, 2016, p.6).

Finalement, bien que le cadre ne soit pas prescriptif au niveau du processus, il mentionne néanmoins qu'un processus de gestion des risques doit intégrer, minimalement, les étapes présentées au tableau 5.31. Or, ces étapes sont pratiquement les mêmes que celles du processus préconisé par la norme ISO31000.

Tableau 5.31 Étapes recommandées par le cadre de GIR du Gouvernement du Canada (Gouvernement du Canada, 2016)

Étape du processus	**Description**
Identification des risques	Les risques sont relevés puis clairement définis. Cette démarche vise tout risque susceptible d'avoir une incidence marquée sur l'atteinte des objectifs de l'organisation (organisation, programme, projet, etc.) selon les paramètres du processus d'identification des risques.
Évaluation des risques	Les risques sont analysés et ordonnés par priorité lors du processus d'évaluation. L'analyse des risques requiert normalement, au minimum, l'évaluation de la probabilité que le risque se produise et des répercussions sur les objectifs le cas échéant. La probabilité et l'incidence sont quantifiées selon les critères établis. L'évaluation des risques porte habituellement sur le risque résiduel (c'est-à-dire le niveau de risque subsistant après l'application des contrôles et des réactions déjà en place), mais elle peut aussi porter sur le risque inhérent (c'est-à-dire le niveau de risque préalable à l'application des contrôles et des réactions déjà en place). L'établissement de l'ordre de priorité des risques devrait tenir compte de la tolérance au risque de l'organisation puisque, dans chacun des cas, le seuil de tolérance relèvera l'écart éventuel entre le niveau de risque évalué et le niveau de risque jugé acceptable.
Réactions aux risques	La réaction aux risques est le processus consistant à sélectionner et à mettre en oeuvre des mesures de réaction à un risque. De manière générale, on opte pour une stratégie de réaction générale (accepter le risque, surveiller le risque, transférer le risque, éviter la menace, réduire la

Étape du processus	Description
	probabilité ou l'incidence de la menace, augmenter la probabilité ou l'incidence d'une occasion, etc.). Le seuil de tolérance au risque devrait déterminer le type et l'envergure de la réaction.
Communication des risques	La communication des risques fait partie intégrante du processus de prise de décisions et se rapporte à au signalement des risques et à la production de rapports sur les risques aux échelons adéquats et au moment opportun afin de soutenir le processus de décisions. La communication s'effectue tout au long du processus de gestion du risque. Il est important que les responsables de la gestion du risque et les personnes susceptibles de subir l'incidence du risque ou associées aux réactions au risque saisissent les critères à l'origine des décisions prises et les justifications motivant les mesures prises. Pour ce faire, il faut communiquer l'information sur le risque à l'intérieur de l'organisation d'une manière utile et efficace au personnel de tous les secteurs d'activités de même qu'à l'extérieur de l'organisation aux clients et aux parties intéressées susceptibles d'intervenir dans les décisions et les actions de l'organisation ou d'en subir les répercussions.
Suivi des risques	Le suivi continu des risques est un aspect essentiel du maintien de la pertinence de l'information sur les risques. Le processus nécessite l'examen régulier de l'information en vue de vérifier si est prise en compte l'incidence des circonstances en constante évolution sur les réactions aux risques en place. Le suivi comprend aussi l'examen des mesures de réaction au risque afin de veiller à ce qu'elles soient mises en oeuvre efficacement et qu'elles produisent les résultats escomptés.

Ainsi, sur le plan de la gouvernance, l’approche de GIR préconisée par le Gouvernement du Canada centralise la gouvernance liée à la GIR (les grands principes et le rôle de supervision de la GIR) au niveau du Conseil du trésor (et son secrétariat), mais décentralise la gestion des risques (donc le processus) vers les responsables des différents ministères et organismes fédéraux. Sur le plan technique, bien qu’il ne propose pas un processus spécifique quant à la gestion des risques, les recommandations qui sont prônées dans le cadre suggèrent une approche qui est très similaire au processus de gestion des risques proposé par la norme ISO31000. Cependant, le cadre ne fait aucunement mention d’une éventuelle intégration des travaux de tous les ministères et organismes à l’intérieur d’un référentiel commun.

5.4.2 Le Modèle de politique en GIR du Gouvernement du Québec

Le Modèle de politique en gestion intégrée des risques du Gouvernement du Québec a été publié en 2022. Il vise précisément les ministères et organismes du Gouvernement du Québec et est construit sur la base de deux cadres de référence en gestion des risques : (1) la norme ISO31000:2018 et (2) le cadre du COSO (version 2017) présenté à la section 5.3.1.

Sur le plan de la gouvernance, le cadre repose sur huit principes directeurs. Ceux-ci sont présentés au tableau 5.32.

Tableau 5.32 Les huit principes directeurs du cadre de GIR du Gouvernement du Québec (Gouvernement du Québec, 2022)

Principe	**Énoncé**
Intégration	La GIR doit être non pas un processus distinct, mais une méthodologie intégrée à tous les processus de l'organisation.
Démarche structurée et globale	La GIR doit s'inscrire dans une démarche structurée et globale afin d'assurer la cohérence et la comparabilité des résultats.
Adaptabilité	La GIR doit être adaptée au contexte interne et externe de l'organisation ainsi qu'à sa mission.
Inclusion	La GIR doit prendre en compte toutes les parties prenantes au moment opportun et valoriser leur expertise et leur point de vue.
Dynamisme	La GIR doit être proactive plutôt que réactive face aux changements touchant l'environnement interne et externe.
Disponibilité de la meilleure information	Le partage de l'information la plus fiable, et communiquée au bon moment, est primordial en GIR.
Facteurs humains et culturels	La GIR est considérablement influencée par le comportement humain et la culture organisationnelle.
Amélioration continue	La GIR doit s'inscrire dans une démarche d'amélioration constante en misant sur l'apprentissage et l'expérience.

Le cadre prévoit aussi un cycle de gestion en quatre phases. Celles-ci sont présentées au tableau 5.33.

Tableau 5.33 Les quatre phases du cycle de gestion du cadre de GIR du Gouvernement du Québec (Gouvernement du Québec, 2022)

Phase	**Énoncé**
Planification	• Des rôles et des responsabilités sont assignés afin de rendre responsables les parties prenantes à l'égard de la GIR. • Les ressources appropriées sont assignées aux activités de GIR les plus critiques qui contribuent à l'accomplissement de la mission.
Mise en oeuvre	• Le plan de GIR est élaboré et mis en oeuvre. • Des mécanismes de suivi des risques identifiés et émergents sont mis en place.
Reddition de comptes	• Un bilan de mise en oeuvre du plan de GIR est effectué en fonction de ses objectifs et des indicateurs qui y sont associés. • Des audits de la GIR sont réalisés.
Amélioration	• Des changements sont apportés en fonction du bilan de mise en oeuvre de la GIR et de l'évolution du contexte interne et externe.

Sur le plan des rôles et des responsabilités, le cadre cible les entités listées au tableau 5.34.

Tableau 5.34 Rôles et responsabilités des différents groupes selon le cadre de GIR du Gouvernement du Québec (Gouvernement du Québec, 2022)

Groupe	**Rôles et responsabilités**
Le sous-ministre, le dirigeant d'organisme ou, le cas échéant, le conseil d'administration	• Approuve la présente politique ainsi que sa mise à jour. • Tient compte des Orientations en matière de GIR dans l'Administration gouvernementale pour mettre en place et développer une fonction de GIR. • Nomme un responsable de la GIR et lui confère les ressources nécessaires à l'accomplissement de ses activités. • Constitue un comité en GIR qui sera soutenu par un comité consultatif, le cas échéant. • Favorise l'instauration d'une culture organisationnelle qui soutient une prise de décision éclairée par la gestion des risques.
La personne responsable de la GIR	• Élabore et met à jour la politique de GIR. • Coordonne l'ensemble des activités en GIR, notamment la mise en oeuvre du plan et les mécanismes de suivi des risques. • Soutient la mise en oeuvre de la GIR, notamment en offrant de l'accompagnement et des outils. • S'assure du développement et du maintien des compétences du personnel en GIR selon les besoins identifiés. • Assure la liaison entre les différentes parties prenantes (ex.: comités de GIR, intervenants internes et externes). • Propose, en collaboration avec les parties prenantes, des seuils de tolérance au comité de GIR pour approbation. • Appuie les propriétaires de risques dans le choix, la mise en oeuvre et le suivi des mesures d'atténuation sous leur responsabilité. • Fait rapport périodiquement au comité de GIR sur la mise en oeuvre du plan de GIR et sur les mécanismes de suivi des risques.
Le comité de GIR (Comité de direction ou comité de gestion)	• Est composé du sous-ministre et des sous-ministres associés ou adjoints ou du dirigeant d'organisme et des vice-présidents (ou leurs équivalents). • Approuve les seuils de tolérance ainsi que le profil de risque. • Détermine les actions afin d'améliorer le plan ainsi que les mécanismes de suivi de GIR sur la base des rapports et des recommandations en GIR. • Peut se doter d'un comité consultatif composé de gestionnaires propriétaires des risques.
Le comité consultatif (si constitué)	• Appuie les propriétaires de risques dans le choix, la mise en oeuvre et le suivi des mesures d'atténuation sous leur responsabilité. • Propose au comité de GIR des seuils de tolérance ainsi qu'un profil de risque. • Examine les rapports de mise en oeuvre et de suivi et soumet des recommandations au comité de GIR.
La personne ou l'unité propriétaire de risques	• Détermine les mesures d'atténuation des risques dont elle est responsable, avec les parties prenantes concernées, y compris les comités de GIR et les unités administratives contribuant à ces mesures. • S'assure de la reddition de comptes et du suivi des mesures d'atténuation des risques sous sa responsabilité.
Le ou la gestionnaire	• Intègre la GIR dans ses opérations. • Informe ses supérieurs des nouveaux risques dans son secteur d'activité et met en place des mesures pour les atténuer.
Les employés	• Informent les gestionnaires des éléments de risque dont ils ont connaissance. • Peuvent être appelés à participer à des activités d'appréciation ou de traitement des risques.
Le ou la responsable de la fonction d'audit interne	• Examine l'efficacité de la fonction de GIR ou de l'une de ses composantes. • Formule des recommandations en vue de contribuer à son amélioration.

Ainsi, le cadre du Gouvernement du Québec est très similaire à celui du Gouvernement du Canada. Sur le plan de la gouvernance, il centralise la gouvernance liée à la GIR (les grands principes et le rôle de supervision de la GIR) au niveau du sous-ministre, de la direction d'organisme ou de son conseil d'administration), mais décentralise la gestion des risques (donc le processus) vers les responsables des différents ministères et organismes provinciaux. Sur le plan de la dimension technique des risques, comme le cadre est basé sur la norme ISO31000, il propose exactement le même processus que celui présenté à l'article sur les défis liés à la gestion des risques émergents (figure 3.1). Toutefois, comme le cadre de gouvernance du Gouvernement du Canada, le cadre ne mentionne aucunement une éventuelle intégration des travaux de tous les ministères et organismes à l'intérieur d'un référentiel commun.

5.4.3 Les Lignes directrices sur la GIR de l'Autorité des Marchés Financiers (AMF)

Les Lignes directrices sur la gestion intégrée des risques de l'AMF (AMF, 2015) ciblent spécifiquement les institutions financières faisant affaire au Québec. S'appuyant sur les principes fondamentaux et orientations publiés par le Comité de Bâle sur le contrôle bancaire (Banque des règlements internationaux, 2012) et l'Association internationale des contrôleurs d'assurance (International Association of Insurance Supervisors [IAIS], 2013), le cadre de l'AMF fournit aux institutions financières des lignes directrices qui énoncent clairement les attentes de l'AMF (envers ces institutions) en matière de GIR.

Sur le plan de la gouvernance, le cadre s'articule autour de quatre principes directeurs. Ceux-ci sont présentés au tableau 5.35.

Tableau 5.35 Les quatre principes directeurs du cadre de GIR de l'AMF (AMF, 2015)

Principe	**Énoncé**
Gestion intégrée des risques	L'Autorité s'attend à ce que l'institution financière effectue une gestion intégrée de ses risques qui soit supportée par des stratégies, politiques et procédures lui permettant d'identifier, d'évaluer, de quantifier, de contrôler, d'atténuer et de suivre adéquatement les risques importants.
Appétit pour le risque, niveaux de tolérance aux risques et limites	L'Autorité s'attend à ce qu'une institution financière établisse et maintienne un énoncé global décrivant qualitativement et quantitativement son appétit pour le risque. Elle s'attend également à ce que l'institution définisse clairement ses niveaux de tolérance aux risques les plus importants et s'assure de les intégrer dans ses opérations, en lien avec ses politiques et procédures de gestion de risques.

Principe	Énoncé
Gouvernance de la gestion intégrée des risques	L'Autorité s'attend à ce que le cadre de gestion intégrée des risques d'une institution financière soit soutenu par une solide structure de gouvernance, laquelle devrait permettre notamment de définir clairement les rôles et responsabilités des différents intervenants impliqués dans la gestion des risques.
Cadre dynamique et évolutif de la gestion intégrée des risques	L'Autorité s'attend à ce que l'institution financière mette en place un cadre lui permettant de gérer adéquatement l'ensemble de ses risques en fonction de son appétit pour le risque. Ce cadre devrait être dynamique, évolutif et mis en place en considérant la nature, la taille et la complexité des activités propres à l'institution.

Sur le plan des rôles et des responsabilités, le cadre cible principalement trois groupes : (1) le conseil d'administration, (2) la haute direction et (3) le chef de la gestion des risques. Le tableau 5.36 présente les rôles et les responsabilités de ces trois groupes.

Tableau 5.36 Rôles et responsabilités des différents groupes selon le cadre de GIR de l'AMF (AMF, 2015)

Groupe	Rôles et responsabilités
Conseil d'administration	• Approuver les stratégies en lien avec l'appétit pour le risque de l'institution. • Assurer la mise en place, par la haute direction, de politiques visant à déterminer et maintenir le niveau approprié de capital en fonction des risques et des objectifs stratégiques de l'institution. • Examiner et approuver le cadre de gestion des risques, ainsi que la mise en place des stratégies pour le soutenir. • Examiner et approuver les politiques mises de l'avant, lesquelles fixent les règles d'acceptation, de surveillance, de gestion et de signalement des risques auxquels l'institution est exposée. • Veiller à ce que la haute direction ou, le cas échéant, le chef de la gestion des risques produise une reddition de comptes régulière sur les risques auxquels l'institution est exposée. • Veiller à ce que la fonction de gestion intégrée des risques de l'institution soit indépendante des opérations courantes, ait un statut et une visibilité suffisante et qu'elle fasse l'objet d'examens périodiques. • Veiller à ce que la compétence et l'expertise collective de ses membres soient suffisantes pour assurer une bonne compréhension, évaluation et quantification des risques. • Veiller à être au fait des différents processus utilisés pour évaluer et quantifier les risques, ainsi que des scénarios utilisés et des simulations de crises effectuées. • Veiller à être informé sur une base régulière de l'évolution des tendances, des risques émergents et des changements importants susceptibles de modifier le profil de risque de l'institution. • Veiller à assurer une communication régulière avec les gestionnaires de risques et le chef de la gestion des risques.
Haute direction	• Mettre en place une politique et des procédures de gestion des risques qui soient adaptées au profil de risque et au plan stratégique de l'institution financière et voir à ce qu'elles soient mises en oeuvre à tous les paliers de l'institution de façon efficace et efficiente. • Attribuer aux personnes appropriées la responsabilité de suivre et de contrôler tous les risques importants dans le respect des stratégies adoptées. • Aligner la gestion de ses risques aux objectifs de création et de préservation de valeur de l'institution, ainsi qu'aux processus d'affaires ou secteurs particuliers où ces risques sont les plus susceptibles de se matérialiser.

Groupe	Rôles et responsabilités
	• Évaluer et s'assurer de tenir compte de l'incidence potentielle des risques identifiés sur les stratégies, la conformité de l'institution et l'intégrité de l'information financière. • Identifier les risques en vue d'établir un ordre de priorité en tenant compte de leur ampleur s'ils se matérialisaient. • Établir des modalités de communication et de recours aux niveaux hiérarchiques supérieurs en réponse à la matérialisation des risques, à l'efficacité des contrôles et aux changements susceptibles de survenir au profil de risque de l'institution financière. • Mettre en place un système de rémunération efficace afin d'éviter que des pratiques risquées soient encouragées, par exemple, la recherche de rendements plus élevés par la prise de positions spéculatives.
Chef de la gestion des risques	• Promouvoir une culture du risque par le biais de la considération et l'intégration des risques dans les décisions stratégiques. • Mettre en place le cadre de GIR et des stratégies de gestion des risques en utilisant notamment l'expertise des gestionnaires de risques des divers paliers de l'institution. • Discuter avec les principaux gestionnaires de secteurs d'affaires sur leurs expositions aux risques plus considérables, dans le but de s'assurer que leurs pratiques soient conformes au cadre de gestion de risques. • Communiquer aux parties intéressées les objectifs d'allocation optimale de capital en fonction de l'ensemble des risques et de l'appétit pour le risque. • Exercer un rôle-conseil auprès des membres de la haute direction et du conseil d'administration. • Éduquer la haute direction et le conseil d'administration sur les enjeux et les interrelations entre les objectifs stratégiques, la position de solvabilité et le cadre de gestion des risques, notamment via les dispositifs d'évaluation des risques et du capital de l'institution. • Prendre les mesures visant à atténuer des risques qui pourraient être néfastes pour l'institution.

Au-delà de ces principes, le cadre transfère entièrement aux institutions financières la responsabilité de voir comment ces principes doivent être mis en oeuvre :

> « L'Autorité reconnaît que la mise en oeuvre d'un cadre de gestion des risques est largement tributaire de la nature, de la taille et de la complexité des activités de l'institution financière. Ainsi, il appartient à cette dernière de mettre en place des stratégies, des politiques et des procédures adéquates afin de gérer ses risques de façon efficace et efficiente en regard des attributs qui lui sont propres » (AMF, 2015, p.9).

En ce qui concerne la dimension technique du risque, le cadre n'impose pas une approche particulière. Néanmoins, comme les cadres canadien et québécois, le cadre de l'AMF prône une approche qui est très similaire au processus de gestion des risques proposé par la norme ISO31000 :

> « …la gestion intégrée des risques implique l'identification des risques importants auxquels l'institution financière est confrontée, leur évaluation, leur quantification, leur contrôle, leur atténuation et leur suivi rigoureux. Elle permet d'identifier les événements susceptibles d'affecter l'institution au-delà des limites de son appétit pour le risque » (AMF, 2015, p.3).

Ainsi, le cadre de l'AMF est très similaire aux cadres du Gouvernement du Canada et du Gouvernement du Québec. Il formule une série de lignes directrices pour les institutions financières qui mentionnent ce qui devrait être fait, mais leur laisse entièrement le soin et la responsabilité de déterminer comment celles-ci doivent être mises en place dans l'organisation, en fonction de ses caractéristiques propres.

5.5 Analyse critique

La revue de la littérature montre qu'il existe plusieurs éléments d'intérêt disponibles aux grandes organisations qui souhaiteraient mettre en place la GIR, que ce soient des outils, des normes, des standards, des cadres de référence ou bien des guides ou des lignes directrices. Même si certains de ces éléments d'intérêt ne concernent pas spécifiquement la GIR, ils peuvent être adaptés pour cela par les grandes organisations qui souhaiteraient s'en inspirer.

La revue de la littérature montre aussi que la plupart des cadres reposent sur la même structure, essentiellement composée de deux volets : (1) un volet concernant la dimension « gouvernance » de la GIR (c'est-à-dire associé au partage des rôles et des responsabilités des acteurs en lien avec la gestion des risques) et (2) un volet concernant la dimension « technique » de la gestion des risques, donc associé au processus de gestion des risques (c'est-à-dire l'identification, l'analyse, l'évaluation des risques, etc.).

Concernant le premier volet, les différents cadres établissent assez clairement que la GIR doit reposer sur un cadre réglementaire précis composé d'un ensemble de politiques, de directives, de processus, etc. Ils font également ressortir l'importance de clarifier les rôles et les responsabilités des principaux acteurs en lien avec la mise en oeuvre de ces cadres ou en lien avec le processus de gestion des risques qu'ils préconisent. Certains sont moins détaillés, d'autres le sont plus, mais en définitive, on comprend bien que ces cadres comportent plusieurs composantes et que celles-ci doivent être sous la responsabilité de différents acteurs. Cependant, on remarque que ces cadres sont établis selon une vision très hiérarchique de la GIR. Ainsi, ils établissent une gouvernance très « verticale » de la GIR, ce que l'on pourrait appeler « l'intégration stratégique » de la gestion des risques, mais ne semblent pas du tout considérer la problématique de la gouvernance associée à l'axe horizontal de la GIR, ce que l'on pourrait appeler « l'intégration transversale » de la gestion

des risques (i.e. l'intégration des travaux de toutes les UF responsables des AGR). Ainsi, qu'en est-il des rôles et des responsabilités des UF responsables des AGR ? Aucun des cadres analysés dans la revue de la littérature ne le mentionne. Or, les travaux avec l'organisation partenaire ont montré que l'enjeu de la GIR ne se situe pas réellement au niveau de son intégration verticale (tous comprennent très bien où se situent les rôles et les responsabilités entre les différents niveaux organisationnels), mais que c'est surtout au niveau de l'axe horizontal que les besoins en gouvernance sont les plus grands. Cela, dans le but d'assurer la coordination, la complémentarité et la cohérence des décisions et des actions de ces acteurs.

Un autre élément qui ressort de la revue de la littérature concerne la mise en oeuvre de la GIR. À cet effet, ces cadres sont établis selon une suite de principes et de lignes directrices qui mentionnent ce qui devrait être fait, et nul ne peut être contre la vertu, mais ils ne mentionnent pas comment le faire. Ils supposent donc, de manière intuitive, que les individus au sein des organisations, et plus spécifiquement au sein des conseils d'administration ou des hautes directions, auront toutes les compétences et les connaissances requises pour le faire, alors que cela n'est pas du tout garanti. En effet, avec la complexité croissante de nos sociétés modernes, des organisations, des systèmes et des risques émergents, la responsabilité de la gestion des risques dans les grandes organisations doit être assignée à des personnes ayant les compétences, les connaissances et l'expertise appropriées, donc, à des personnes spécifiquement formées dans le domaine de la gestion des risques. Prendre pour acquis que les personnes les plus haut placées dans l'organisation sont les mieux placées pour analyser et évaluer les risques et prendre les décisions qui s'y rattachent est donc une erreur. Plutôt, une organisation devrait faire en sorte que les personnes responsables de la gestion des risques, quel que soit leur niveau hiérarchique, puissent travailler ensemble à identifier et analyser les différents risques auxquels l'organisation est confrontée et faire les recommandations pertinentes qui s'imposent afin de permettre à la haute direction et au conseil d'administration de prendre des décisions plus avisées quant à la gestion des risques ou faire des choix plus éclairés sur toute autre question, mais en tenant compte des risques.

En outre, bien que le concept de GIR soit généralement bien défini par la plupart des cadres analysés, il semble que la transposition du concept au niveau pratique en réduise la portée. En effet, ceux-ci semblent considérer que la gestion des risques devient intégrée lorsque toutes les parties prenantes participent au même processus de gestion des risques. Ainsi, tous les cadres mentionnent l'importance de la communication et de la consultation à toutes les étapes du processus. Or, comme

il l'a été démontré au chapitre 3, la GIR, ce n'est pas de faire en sorte que tous participent au même processus de gestion des risques, mais plutôt de faire en sorte que les ICII sur les risques soient mises en commun afin d'obtenir une vision plus holistique des risques auxquels est confrontée l'organisation et d'assurer la coordination, la complémentarité et la cohérence des décisions qui sont prises et des actions qui sont posées par toutes les parties prenantes impliquer dans la gestion des risques (ce qu'on pourrait qualifier d' « enjeu de la transversalité » de la GIR). Cela, tout en reconnaissant que chacune de ces parties prenantes puisse avoir ses propres processus et façons de faire relativement à la gestion de ces risques. Sur ce point, les cadres canadien et québécois, incluant celui de l'AMF, s'inspirent davantage du concept même de GIR que les autres cadres de gestion analysés puisqu'ils établissent une gouvernance centralisée de la GIR, mais ils décentralisent, vers les acteurs concernés, la gestion des risques elle-même (c'est-à-dire, le processus). Cela dit, ces cadres ne mentionnent pas comment les résultats de tous ces processus doivent ensuite être intégrés (agrégés et corrélés). D'ailleurs, ils ne semblent pas du tout considérer ce point. Si cela peut se justifier dans un contexte comme celui de l'AMF, dont le rôle est de s'assurer que chaque institution financière (indépendamment des autres) adopte de saines pratiques de GIR, cela l'est moins dans le contexte des gouvernements du Canada et du Québec, dont l'objectif est d'assurer la coordination, la complémentarité et la cohérence des décisions et des actions de tous les ministères et organismes en regard des risques auxquels le gouvernement, en tant qu'organisation, et la population, par ricochet, sont confrontés. Comme l'a démontré la crise sanitaire de la COVID-19, même si chaque entité au sein du gouvernement fait sa propre gestion des risques à l'interne et que cela semble *a priori* fonctionner (sur papier ou lors d'exercices de simulation), l'enjeu est tout autre lorsque plusieurs ministères et organismes doivent répondre à une même situation de problème qui les affecte tous transversalement. Si les priorités n'ont pas été établies de manière globale et concertée et que les rôles et les responsabilités des acteurs impliqués dans l'intervention commune n'ont pas été clairement établis, alors forcément il en résultera une incohérence dans le processus de réponse qui pourrait conduire à des actions décousues de la part de ces acteurs, voire même créer des tensions entre ceux-ci qui seraient fortement contre-productives en regard de la prise en charge globale de la situation de risque. Les approches comme celle prévue par les cadres de GIR du Gouvernement du Canada et du Gouvernement du Québec sont donc, en soi, insuffisantes puisqu'elles ne résolvent pas d'emblée cet enjeu de la transversalité.

Sur le plan de la dimension technique des risques, la revue de la littérature a permis de constater que la plupart des cadres analysés proposent des processus très similaires à celui préconisé par la norme ISO31000. Le seul cadre à proposer une approche différente est le *Cybersecurity framework v2.0* du NIST qui est davantage structuré selon les dimensions de la sécurité civile (prévention, préparation, intervention et rétablissement). En ce sens, cette structuration est intéressante puisque dans les grandes organisations, dont l'organisation partenaire, ces dimensions sont la plupart du temps sous la responsabilité d'UF différentes, ce qui, dans un contexte d'intégration, permet de délimiter les frontières des rôles et des responsabilités des UF mieux qu'on ne serait capable de le faire à partir de la structuration du processus de gestion des risques. De plus, sans revenir sur tous les constats établis au chapitre 3, les cadres qui reposent principalement sur le processus de gestion des risques recommandé par la norme ISO31000 et qui demandent d'établir un seuil de tolérance des risques, de les quantifier en utilisant des approches quantitatives (comme celles présentées dans la norme IS031010, par exemple) et de les évaluer en regard de ce seuil sont beaucoup moins adaptés aux risques émergents. Sur ce point spécifique, le cadre COSO se distingue au niveau de l'application du processus de la norme ISO31000. En interprétant le risque comme étant l'effet de la non-atteinte d'un objectif d'affaires sur la mission de l'organisation, ce cadre adopte, dans les faits, une approche tous risques qui est davantage arrimée à la nouvelle définition du risque adoptée par la norme ISO31000:2018 et qui est aussi davantage en adéquation avec les défis liés à la gestion des risques émergents puisqu'elle évacue le besoin d'identifier des aléas et de leur assigner une probabilité d'occurrence.

Finalement, un autre élément qui ressort de l'analyse de ces cadres est que la plupart semblent sous-estimer la dimension humaine de la gestion des risques, c'est-à-dire, toute la question liée aux perceptions individuelles des acteurs en regard des risques. Ces cadres mettent donc énormément d'emphase sur les dimensions gouvernance et technique de la gestion des risques, mais semblent considérer sa dimension humaine comme un problème secondaire dont la résolution se résume à impliquer toutes les parties prenantes dans le processus de gestion des risques. Or, dans le cas de la GIR, et plus spécifiquement dans le contexte des grandes organisations où plusieurs acteurs sont impliqués dans la gestion des risques, cette question de la perception des risques est un enjeu qui doit absolument être adressé de front, surtout dans un contexte de risques émergents empreint d'incertitude et d'ambiguïté. À cet effet, parmi les cadres analysés, celui de l'IRGC est le seul à mentionner la problématique de la perception des acteurs et des biais cognitifs résultant de cette

perception dans les analyses de risques et à proposer de travailler au niveau du développement de l'intelligence situationnelle de ces acteurs afin de réduire les effets de ces perceptions, corroborant ainsi d'ailleurs les constats ressortant de l'article 2 sur les défis liés à la gestion des risques émergents. Sans pour autant proposer de solution à cette problématique, en soulignant les lacunes en matière de gouvernance (i.e. déficits de gouvernance) et en suggérant d'ajuster la méthode d'analyse en fonction des types de risques (simples, complexes, incertains, ambigus) et des connaissances disponibles, le cadre de l'IRGC permet d'alimenter la réflexion et de sensibiliser sur l'importance d'intégrer ces facteurs dans les analyses de risques.

Ainsi, la revue de la littérature a permis d'identifier certaines opportunités intéressantes au niveau des trois dimensions de la gestion des risques. Sur le plan de la gouvernance, il ressort de la revue de la littérature qu'il y a un manque au niveau de la gouvernance reliée à l'intégration transversale de la GIR, c'est-à-dire au niveau des rôles et des responsabilités des UF responsables des AGR. Sur le plan de la dimension technique de la GIR (donc sur le plan de la gestion des risques en tant que processus), il ressort de la revue de la littérature que la plupart des cadres analysés recommandent l'approche traditionnelle de gestion des risques qui demande de quantifier les risques et de les évaluer en fonction d'une valeur correspondant à un seuil de tolérance. Or, comme il l'a été démontré dans l'article 2 sur les défis liés à la gestion des risques émergents (et comme le mentionne aussi l'IRGC dans son cadre de gouvernance (tableaux 5.9 et 5.10)), cette approche est insuffisante pour aborder les risques émergents. Finalement, concernant la dimension humaine des risques reliée à la prise en compte des effets des perceptions individuelles des acteurs dans les analyses de risques, aucun cadre ne prend réellement en compte cette dimension (outre le cadre IRGC qui ne fait que la mentionner).

Ainsi, ces travaux de recherches viseront à développer un cadre de gouvernance pour la GIR qui intègre les trois dimensions de la gestion des risques, dans un contexte qui cible davantage les grandes organisations et les risques émergents. Pour cela, plutôt que d'utiliser le concept de risque issu des mathématiques, ces travaux utiliseront le concept de risque basé sur l'incertitude. Dans ce paradigme, où le risque est associé à une incertitude, réduire le risque revient donc à réduire l'incertitude, donc à accroître la connaissance. Pour y arriver, les travaux proposent d'adapter le concept d'EC développé par le CRP lors de ses travaux sur DOMINO afin de permettre aux acteurs responsables de la GIR dans les grandes organisations de mettre en commun les ICII sur les risques réparties à travers l'organisation. Cette mise en commun devra permettre à ces acteurs de co-

construire une connaissance collective nouvelle transversale (transdisciplinaire) sur les risques qui leur permettra de développer leur ISP, c'est-à-dire développer une RMC des risques auxquels l'organisation est confrontée et mettre en place un COC pour leur gestion. Ainsi, en intégrant les trois dimensions de la GIR (gouvernance, technique et humaine) et en combinant les concepts d'EC, d'incertitude, de gouvernance, de socioconstructivisme et d'ISP, ces travaux présentent une avenue tout-à-fait originale d'adresser la problématique de la GIR dans les grandes organisations.

CHAPITRE 6 ARTICLE 3 : A GOVERNANCE FRAMEWORK FOR ACHIEVING TRANSVERSAL AND STRATEGIC INTEGRATION OF RISK MANAGEMENT IN LARGE ORGANIZATIONS[25]

Morabito, L. et Robert, B. (). 'A governance framework for achieving transversal and strategic integration of risk management in large organizations', *Int. J. Decision Sciences, Risk and Management*, Accepté pour publication le 29 mai 2025.

6.1 Mise en contexte et présentation de l'article

Le risque est une notion qui peut paraître complexe en raison de son côté abstrait. Il en existe plusieurs définitions selon les domaines d'application et chaque individu a aussi sa propre vision (perception, interprétation) de ce qu'est le risque (Chionis et al. 2022). Ce constat est d'ailleurs ressorti dès les premières rencontres avec l'équipe de projet au sein de l'organisation partenaire. Bien que travaillant tous dans le domaine de la gestion des risques et pour la même organisation, et bien qu'étant tous des experts chevronnés dans leur domaine respectif, chaque membre de l'équipe de projet avait, en fonction de son domaine de spécialité, une vision différente de ce qu'est le risque. Ainsi, les experts en continuité des affaires et ceux en mesures d'urgence avaient une vision du risque davantage portée sur les impacts, alors que les experts en sécurité physique et protection des actifs et ceux en gestion des accès avaient, pour leur part, une vision du risque davantage portée sur les aléas. Or, ces divergences de perceptions au niveau du concept de risque faisaient en sorte qu'il y avait une forme de dissonance au niveau des échanges qui était flagrante pour le chercheur, mais qui ne semblait pas aussi évidente pour les différents experts. Ainsi, tous utilisaient les mêmes mots, mais avec une interprétation différente de la signification de ces mots, avec pour résultat final une forme d'inconsistance au niveau du discours global.

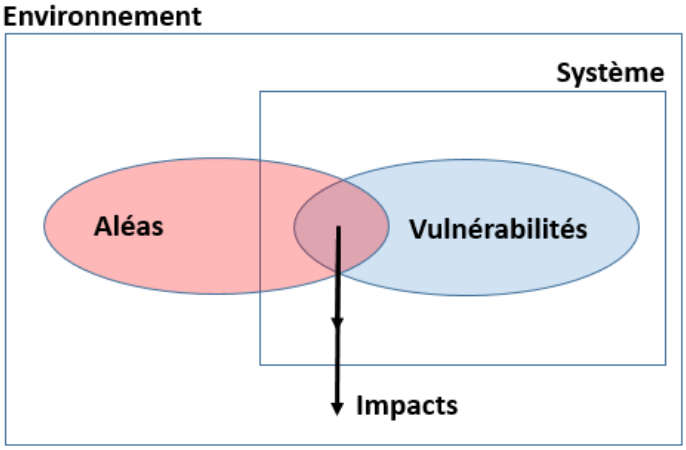
Or, pour assurer le succès de toute action ou initiative transverse (ou collective), non seulement une volonté (ou une intention) commune de se lancer dans cette initiative est requise, mais une

[25] Même si le titre de cet article suppose qu'il aborde le cadre de gouvernance dans son entièreté, cet article aborde uniquement la dimension « gouvernance » de la GIR, donc le premier pilier du cadre de gouvernance proposé dans cette thèse.

compréhension et une vision communes de la situation à résoudre (donc, de la problématique) sont absolument essentielles (Agaisse et al. 2018). La première étape au niveau de toute initiative de coopération impliquant plusieurs parties prenantes est donc d'adopter un langage commun et une compréhension commune des concepts abordés afin d'harmoniser les discussions et les réflexions au niveau des acteurs impliqués. Dans ce sens, et en lien avec le premier objectif spécifique de ces travaux de recherche (et première composante d'un EC), l'objectif de ce chapitre est de définir le référentiel commun qui permettra de fédérer les acteurs des différentes UF responsables des AGR autour une RMC (ou vision commune) des concepts de risque et de GIR et qui permettra de fournir à ces acteurs une compréhension commune du rôle que chacun d'eux joue dans la gestion des risques et d'établir un CRC pour leurs actions. L'établissement du référentiel commun est essentiel afin d'assurer la coordination, la complémentarité et la cohérence des décisions prises et des actions posées par chaque acteur impliqué dans l'initiative commune.

L'article présenté ci-après présente donc le référentiel commun pour la GIR (premier pilier du cadre de gouvernance pour la GIR chez les organisations de grande ampleur qui est proposé dans cette thèse). Reposant sur les constats issus de l'analyse critique de la revue de la littérature, l'article montre que la GIR présente un double défi d'intégration : un défi d'intégration horizontal (associé à la dimension transversale de la GIR), pour permettre l'arrimage entre les différentes UF responsables des AGR, et un défi d'intégration verticale (associé à la dimension stratégique de la GIR), pour permettre l'arrimage entre les niveaux stratégique, tactique et opérationnel de l'organisation (en lien avec la mission, les objectifs et les opérations de l'organisation). Pour résoudre cette double intégration, l'article propose un référentiel commun constitué d'une RMC (servant à atteindre l'objectif d'intégration horizontale de la GIR) et d'un CRC (servant à atteindre l'objectif d'intégration verticale de la GIR).

Concernant la RMC, les travaux avec l'organisation partenaire ont permis d'adopter un modèle de risque transversal à l'organisation. Ce modèle repose sur le concept de risque basé sur le triptyque aléas/vulnérabilités/impacts. Ce concept avait été utilisé par le CRP dans le cadre de ses travaux sur la résilience (Robert et al., 2013 ; Robert et Morabito, 2013) et également par le Ministère de la Sécurité publique du Québec (MSP) (Gouvernement du Québec, 2008a). La figure 6.1 montre ce concept de risque.



$$R = f(Aléas, Vulnérabilités\ du\ système, Impacts)$$

Figure 6.1 Concept de risque basé sur le triptyque aléas/vulnérabilités/impacts (adaptée de Robert et Morabito, 2013)

Dans cette optique, un risque existe lorsqu'il y a présence dans un même environnement et au même moment d'un aléa[26] et d'un système qui lui est vulnérable[27]. Dans ce cas, le risque devient alors la mesure de la valeur (ou du poids) de cet aléa en regard de sa possibilité d'occurrence[28] dans l'environnement considéré et de ses conséquences sur le système étudié. Cette définition du risque présente l'intérêt de permettre l'utilisation des probabilités (ou fréquences) d'occurrences lorsqu'elles sont disponibles (dans un contexte de risque traditionnel), mais, selon les objectifs visés et les informations (ou données) disponibles, offre l'opportunité de centrer l'analyse du risque indépendamment sur les aléas, les vulnérabilités ou les impacts. Cela est d'autant plus intéressant dans le contexte de la gestion des risques émergents pour lesquels les informations sur les aléas et

[26] Un aléa est un événement aléatoire, donc imprévisible (Le Robert en ligne, 2025). Par imprévisible, on entend que l'aléa peut se produire, ou non, à l'intérieur de l'environnement que l'on considère. Le terme aléa n'a donc ni connotation négative, ni positive. Cependant, dans le domaine des risques, le terme aléa est souvent utilisé comme un synonyme de danger ou de menace. On associe donc l'aléa à « un phénomène, une manifestation physique ou une activité humaine susceptible d'occasionner des pertes en vies humaines ou des blessures, des dommages aux biens, des perturbations sociales et économiques ou une dégradation de l'environnement » (Gouvernement du Québec, 2008b, p. 6). Dans ce contexte, où l'on ne tient compte que des impacts négatifs des aléas (i.e. les aléas ne sont associés qu'à des événements pouvant avoir des conséquences négatives), on utilise parfois, dans la littérature, l'expression « risque aryétique » (Jousse, 2009).

[27] La vulnérabilité représente une faiblesse d'un système. Il s'agit d'une « condition résultant de facteurs physiques, sociaux, économiques ou environnementaux, qui prédispose les éléments exposés à la manifestation d'un aléa à subir des préjudices ou des dommages » (Gouvernement du Québec, 2008b, p. 8). Cette faiblesse peut être intrinsèque au système (ex.: un système électrique vulnérable à l'eau) ou être le fruit d'une mauvaise conception ou d'une dénaturation/détérioration du système (ex.: une pièce d'équipement mal fabriquée ou mal entretenue). La vulnérabilité d'un système varie en fonction du temps (paramètre dynamique).

[28] Qu'est-ce qui distingue la probabilité d'occurrence de la fréquence d'occurrence ? Un événement est probable s'il a des chances de survenir. Cependant, cela ne signifie pas qu'il se produira. Un événement arrive à une fréquence donnée (ou de manière périodique) lorsque, statistiquement, il est possible de montrer que l'événement se produit de manière récurrente sur une certaine période de temps. Par exemple, selon Environnement et Changements Climatiques Canada, la probabilité qu'un individu soit frappé par la foudre au Canada est inférieure à 0,0001%, soit 1/1 000 000. Par contre, la fréquence à laquelle la foudre tue un individu au Canada est de 1 personne tous les 121,7 jours, soit 2 à 3 personnes par année (Mills, 2020).

leurs impacts potentiels sont plus difficilement disponibles (comme mentionnés au chapitre 3). Ce modèle permet donc d'intégrer à la fois les risques traditionnels (auxquels les organisations font majoritairement face) et les risques émergents (plus difficile à cerner). Également, cette définition du risque présente un intérêt particulier au niveau de la mise en application du concept de GIR dans les grandes organisations. En effet, comme les composantes du risque (aléas, vulnérabilités et impacts) sont souvent traitées par des UF différentes, pouvoir les scinder offre l'opportunité de laisser à chaque UF son champs d'expertise, tout en rendant possible une intégration de leurs travaux (qui demeure l'objectif fondamental visé par la GIR). La figure 6.2 dans l'article qui suit montre comment ce concept de risque a été traduit en un modèle d'agrégation pour la GIR.

Concernant le CRC pour les acteurs et leurs actions, les travaux avec l'organisation partenaire ont permis d'adopter une structure documentaire uniforme à l'ensemble des UF responsables des AGR. La figure 6.4 dans l'article qui suit montre cette structure documentaire. Celle-ci inclut l'ensemble des composantes clés de la gouvernance illustrées à la figure 3.3, et que l'on retrouve aussi au niveau des cadres de gestion des risques analysés dans la revue de la littérature, mais ajoute une composante intéressante que l'on ne retrouve pas dans ces cadres : les chartes de programmes. Celles-ci seront aussi présentées dans l'article.

Finalement, l'article ouvre sur deux constats. Le premier de ces constats veut que l'implantation d'un cadre de gouvernance pour la GIR ne puisse fonctionner que si une structure de coopération favorisant les intégrations transversale et stratégique de la GIR est mise en place dans l'organisation et si une entité au sein de l'organisation se voit confier le mandat de la GIR. Ce constat ouvre la voie au deuxième pilier du cadre de gouvernance (et deuxième composante d'un EC), la structure de coopération, abordé au chapitre 7. Le deuxième constat veut que la pertinence d'un cadre de gouvernance pour la GIR ne puisse être démontrée que s'il permet de créer de la valeur en permettant de générer des connaissances collectives nouvelles et transversales (transdisciplinaires) qui ne pourraient être autrement générées. Ce constat ouvre la voie au troisième pilier du cadre de gouvernance (et troisième, et dernière, composante d'un EC), le modèle d'agrégation des ICII sur les risques, abordé au chapitre 8.

6.2 Abstract

In large organizations, activities related to risk management (ARM) such as business continuity, physical security or information security are most often conducted in silos, by different organizational units (OUs). To ensure consistency of decisions and actions taken by these OUs, organizations must implement integrated risk management (IRM) governance frameworks. However, many that try come up against major difficulties, despite the resources they dedicate to the effort.

Indeed, most of the frameworks available to organizations require from them, right from the beginning, a certain level of maturity related to IRM which is not always achieved. Hence, there is a need to provide organizations with more simple frameworks that can help them reach a certain level of maturity, so they can eventually explore more comprehensive approaches.

This article aims this objective. It proposes a governance framework for IRM which was established on the basis of empirical work conducted in a large Canadian organization. Resting on two pillars, a shared mental model (SMM) and a common frame of reference (CFR), this framework aims to improve IRM-related governance by focusing on roles/responsibilities of OUs responsible for managing ARM. Simple indicators are also provided so organizations can identify areas requiring improvement.

Keywords: common frame of reference, governance framework, integrated risk management, large organizations, shared mental model.

Reference to this paper should be made as follows: Morabito, L. and Robert, B. (2025) 'A governance framework for achieving transversal and strategic integration of risk management in large organizations', *Int. J. Decision Sciences, Risk and Management*, Vol. x, No. x, pp.xx–xx.

6.3 Introduction

6.3.1 IRM: A summary description

IRM is a crosscutting corporate risk management approach (Bohnert et al., 2019) that is directly related to the concept of risk governance (International Risk Governance Council [IRGC], 2018). It is meant to ensure that all the organizational players who have a role to play in risk management

work together, in a synergistic way, to identify, understand and mitigate risks (Amansou, 2019; Morabito and Robert, 2023b; Salim et al., 2021). The objective of IRM is to centralize the organization's risks into a single, holistic view (Donohue, 2023; Government of Canada [GOC], 2016), thereby supporting its risk-related decision-making processes and ensuring consistency of decisions and actions taken to reduce risks (Morabito and Robert, 2023b).

There are two major aspects to IRM: a governance (or social) aspect and a technical aspect. The governance aspect of IRM is related to how risk management is orchestrated within the organization, that is to say how the roles/responsibilities associated with risk management are distributed across the various OUs responsible for managing ARM; the technical aspect of IRM is related to how the outcome of the work done by these OUs are aggregated/correlated so they can be reflected in key risk indicators (KRIs) capable of providing the organization with an overall portrait of the risks it faces and better supporting its more tactical and strategic decision-making processes (Morabito and Robert, 2023b) – what is called *risk data aggregation and risk reporting* (Basel Committee on Banking Supervision, 2012). This article focuses on the governance aspect of IRM.

6.3.2 The complexity of IRM in large organizations

IRM requires cooperation and coordination from all organizational players who have a role to play in risk management (Amansou and Chaouki, 2019; Jean-Jules and Vicente, 2020). The larger the organization, the more complex the challenge for IRM becomes. In fact, this challenge does not really arise in small organizations. In those cases, only a few people (often a single team) are responsible for managing risks. Therefore, risk management in small organizations is integrated by default. However, in large organizations, which are most often composed of several thousand players within numerous OUs, sometimes distributed among large and widely dispersed geographic areas and characterized by multi-level decision-making (i.e., hierarchical levels), the challenge of cooperation and coordination is much more complex. Indeed, in these cases, risk management is most often divided into multiple ARM, each being under the responsibility of a different OU (Morabito and Robert, 2023b). Examples of ARM include: business continuity, emergency management, physical security, computer security, information security, occupational health and safety, and building management. Thus, in large organizations, IRM must be addressed

by a crosscutting initiative that involves all these OUs and all organizational levels, ranging from top management to operations.

The literature provides organizations with few frameworks for risk management. Some of the best-known ones include the Control Objectives for Information and Related Technologies (COBIT) framework for information technology management and governance (Information Systems Audit and Control Association [ISACA], 2012), the Committee of Sponsoring Organizations (COSO) enterprise risk management framework (COSO, 2004), the IRGC risk governance framework (IRGC, 2017), and the National Institute of Standards and Technology (NIST) risk management framework for information systems and organizations (NIST, 2018b).

Although these frameworks are well organized and quite exhaustive, their implementation in large organizations do present some challenges. First, when analysing these frameworks strictly from a governance lens, one can notice that these are heavily vertically oriented – meaning that roles/responsibilities are mainly segregated/assigned according to the three organizational levels (strategic, tactical and operational) – and they seem to consider that most of the work related to IRM is being done at the board and senior management levels. However, from our experience, the bigger part of the problem related to IRM does not lie in the segregation between role/responsibilities at these three organizational levels (these are actually pretty well understood), but rather in the interdependencies and interactions between the various OUs responsible for managing ARM, what these frameworks do not seem to consider, and which is one of the main objective IRM should strive for.

Another downside of these frameworks is that they are broken down into sets of guidelines that organizations should align too, but they don’t specify how to meet those requirements. Simply put, these frameworks tell very well what to do, but they don’t really tell how to do it. They assume that practitioners within organizations will have the required expertise to implement them, hence leaving it to them to decide how this implementation should be done. However, one must keep in mind that risk management is not the core activity (or primary mission) of most large organizations and that people responsible for managing risk in these organizations are not necessarily seasoned experts in this field. Hence, the issue is not necessarily with the frameworks themselves, but lies more in the fact that they require a certain level of maturity to be reached by the organization (with regard to risk management) before they can be implemented. For an organization that is starting to

implement an IRM framework, this can get quiet overwhelming and create a certain discouragement. Thus, many organizations turn to computer tools such as enterprise risk management tools, thinking that these will do most of the work and they will gain much valuable time. However, this is not the case. Tools can be very efficient to optimize/accelerate certain tasks, but they are not made to compensate for a lack of expertise, nor to circumvent fundamental preliminary steps required when implementing an IRM framework and that are related to the organization's risk management culture. As a result, many organizations that attempt to implement such frameworks/tools come up against major difficulties or simply fail, despite the resources they dedicate to the effort. They view IRM as a technical problem, when in reality, there is a much broader social aspect to it (Jean-Jules and Vicente, 2020), which is specifically what the framework proposed in this article focuses on.

6.3.3 The twofold integration challenge of IRM

IRM-related governance presents a twofold integration challenge: a horizontal (crosscutting) integration challenge, to allow the alignment of the various OUs within the organization; and a vertical (strategic) integration challenge, to allow the alignment of the organization's strategic, tactical and operational decision-making levels (related to its mission, objectives and operations).

The main issue in crosscutting integration stems from the fact that most large organizations are organized according to function (i.e., in silos). Although this structure is well adapted for daily operations, it is less appropriate for addressing crosscutting initiatives that require several OUs to cooperate (Jacob and Michel, 2020). Indeed, in this kind of structure, OUs are relatively independent in their daily operations and there are not necessarily many joint initiatives that demand regular cooperation (Luokkala et al., 2017; Tena-Chollet et al., 2017; Hwang and Yoon, 2020). This means that OUs do not necessarily have a good understanding of other OUs' operations and roles/responsibilities, and that their work is not systematically integrated (Rao, 2007). However, this kind of integration is absolutely necessary to ensure that risks are being consistently managed overall by the organization, through the decisions and actions taken individually by all of its OUs.

Meanwhile, the main issue in vertical integration stems from the fact that large organizations usually have several hierarchical levels, resulting in a great distance between the bottom and top of the hierarchy. On one hand, this distance means that people working at the operational level do

not necessarily have sufficient knowledge of the strategic goals that management is seeking to achieve (i.e., its vision); on the other hand, top management does not necessarily have an accurate understanding of operations and their related challenges (Hamel, 2011). All of this means that the organization's strategic objectives and the actions that are carried out in operations are not always coherently aligned. However, such alignment is crucial so that, on one hand, the organization's strategic objectives, in terms of risk management, can be decentralized to all of its players, down to the operational level, in a coherent way, and, on the other hand, the outcomes of the actions conducted at the operational level can make their way up the hierarchy so they can support tactical and strategic decision-making.

To resolve this twofold integration challenge, the framework proposed in this article rests on two pillars: (1) a SMM and (2) a CFR. The following sections address those two pillars.

6.4 The SMM: Achieving the goal of transversal integration of IRM

Crosscutting integration of IRM aims to allow the various OUs responsible for managing ARM to work in a synergistic way, rather than in silos. The challenge is to instill in these actors a common vision and comprehension of the problem in which they are jointly involved. That is what the SMM is for.

SMMs are representations, usually visual ones, meant to represent a team's joint understanding of something (Palmer, 2023). They refer to the collective understanding among team members of their roles, to ensure everyone is on the same page regarding what needs to be done and how to coordinate their efforts in order to achieve a common goal (Edgar et al. 2021). With regard to the IRM governance framework proposed in this article, the SMM is composed of three elements:

1. An aggregation model that provides OUs a common representation of the concept of risk and enables them to visualize where and how they contribute to risk management;
2. Program charters that precise OUs' missions, objectives and roles/responsibilities with respect to risk management;
3. A mitigation and control measures (MCMs) governance matrix that provides indicators regarding the state of the IRM-related governance associated with the management of MCMs.

The following sections explain in more detail these three elements.

6.4.1 The aggregation model

An organization can be considered as a sociotechnical system made up of several assets. These assets comprise the organization's tangible and intangible property, including information, people and equipment/systems, amongst other (Business Lab, 2022). Assets are used to execute different functions that enable the organization to fulfill its mission, which may be reflected in the provision of a resource (or service) (Robert et al., 2007). Assets present vulnerabilities. These may be inherent in the assets (e.g., electrical equipment is vulnerable to water) or they may be the outcome of a deterioration in their condition due to external (e.g., weather) or internal factors (e.g., lack of maintenance). Meanwhile, threats exist in the assets' environment. They too may be external or internal to the organization and there are different kinds (human, natural, technological and financial/political). When a threat and a vulnerability combine, the result is impacts that may also be either external or internal to the organization.

To reduce risks, organizations deploy various MCMs. These may serve for prevention/protection (to prevent risky situations and protect assets), monitoring/detection (to monitor the environment and detect situations likely to affect assets), or intervention/recovery (to reduce the impacts of a disruptive event or return to normal operations after a failure). Figure 6.2 illustrates this reasoning and depicts the IRM aggregation model proposed in this article, which relies on the risk concept based on the trinity threats/vulnerabilities/impacts.

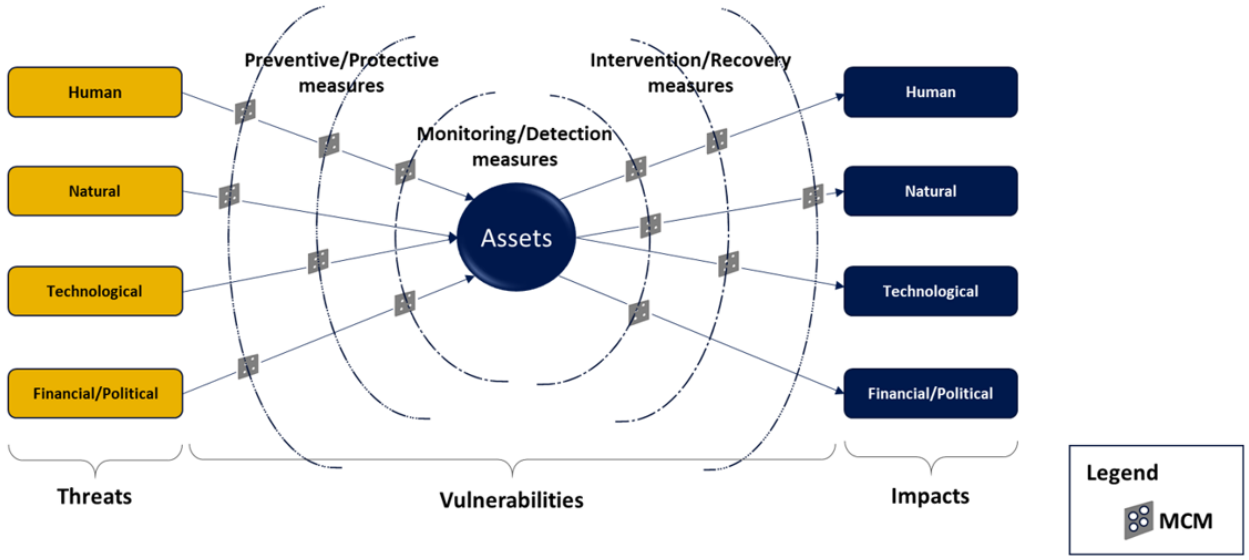


Figure 6.2 Proposed IRM aggregation model

This aggregation model is inspired by a combination of three risk representation models: (1) the bowtie, (2) the what-if, and (3) the defense in depth. The bowtie model is widely used to address technological risks (e.g., explosions, toxic gas clouds) (Center for Chemical Process Safety [CCPS], 2018). The feared event is located in the center of the model. In the aggregation model, the feared event is replaced by the organization's assets. The bowtie model uses security barriers. In the aggregation model, these security barriers are the MCMs and are represented by the what-if model, also known as the Swiss cheese or Reason model (Reason et al., 2006). Since these security barriers are not perfect, they are typically represented as slices of Swiss cheese, where the holes in the slices represent the MCMs' vulnerabilities. Thus, an accident is possible when an alignment of vulnerabilities exists, which makes it possible for a threat to affect an asset and trigger impacts. Finally, the defense in depth model (represented by the concentric half-ellipses around the assets) is widely used in physical (Baker and Benny, 2014) and computer security (United States Department of Homeland Security [US DHS], 2014). It is intended to create a structure with successive layers, where security increases and access privileges decrease as one approaches the organization's most critical assets. In the aggregation model, it allows to consider the various levels of protection, detection and recovery in the event that an MCM fails. As this article focuses on the governance aspect of IRM, it will explain how this model can improve IRM-related governance and provide indicators to target areas requiring improvement.

6.4.2 The program charters

The aggregation model allows to illustrate the main challenge related to IRM in large organizations: several OUs may act upon a given MCM simultaneously. Thus, where one OU may be responsible for identifying the measure to be put in place, another may be responsible for implementing it, a third for funding it, a fourth for operating it, and so on. This all functions as an ecosystem (Whitacker, 2016) in which each OU as a role to play in ensuring MCMs function adequately and they are always proportional to the level of threats and impacts – so that a balance between the three risk parameters is maintained and the risks remain within what the organization considers an acceptable threshold. However, since operations are generally carried out in silos, this results in a situation where each OU has a view of part of the system but no single OU has an overview of the whole system, as figure 6.3 shows.

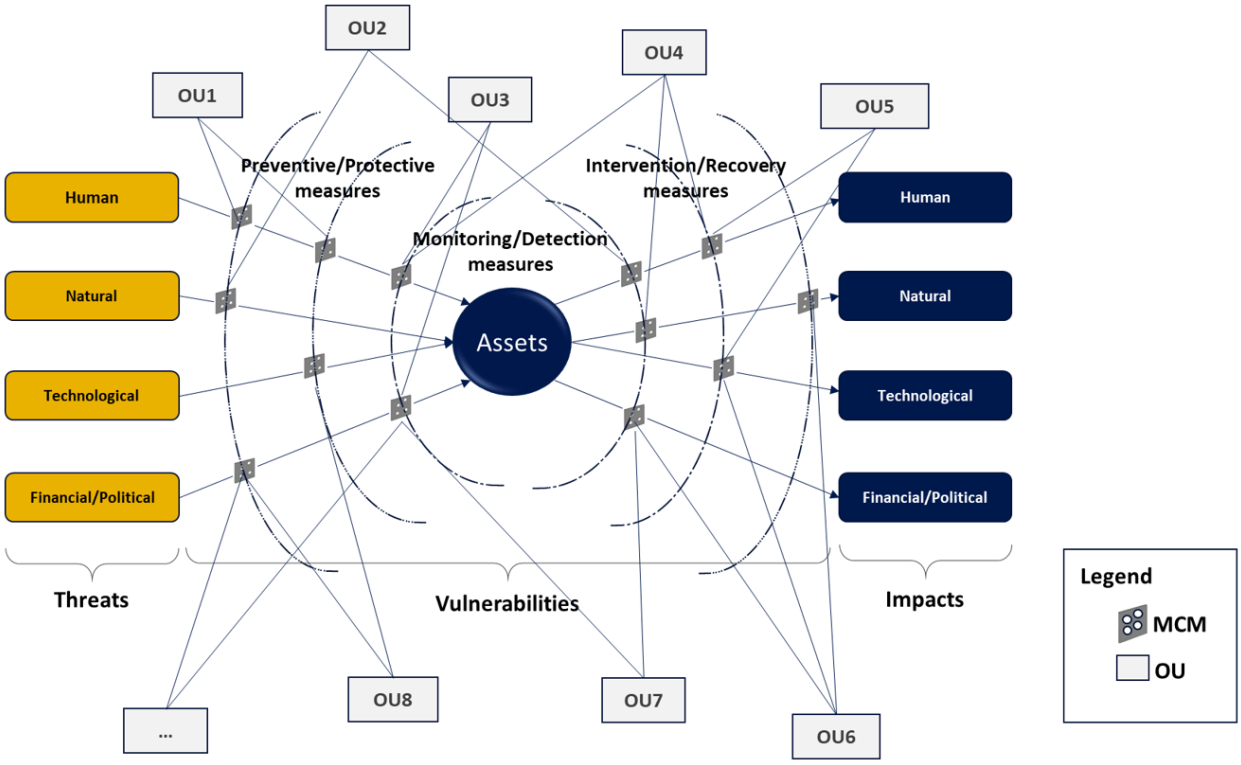


Figure 6.3 Overview of the risk management ecosystem in large organizations

Consequently, a certain ambiguity/confusion, may exist regarding the sharing of roles/responsibilities between OUs. This confusion can lead to erratic communications and a lack of coordination, which in turn can lead to inefficient decision-making, the results of which are especially evident in situations other than normal operations, such as a disruptive event requiring

several OUs to take action. Thus, the first IRM-related governance indicators an organization needs concern the OUs' roles/responsibilities in respect of the various MCMs deployed to mitigate risks.

To this end, each OU must construct a program charter. Inspired by project charters (Project Management Institute [PMI], 2017) and team charters (GOC, 2020), program charters explain how the OUs function and establish how much each one contributes to MCM functioning, and ultimately, to risk management. In its program charter, each OU must clearly set out its mission. The mission corresponds to the OU's reason for existing. It must be expressed in a concise, unambiguous statement, and be aligned with industry standards, guidelines and best practices. For example, for the "Business Continuity" OU, the mission should be based on the international organization for standardization (ISO) standard ISO22301 and should state that the organization can "continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption" (ISO, 2019a). Then, each OU must define its objectives and identify the related MCMs. These objectives must be clearly defined and must cover all aspects related to the OU's mission. Finally, the program charter must mention how roles/responsibilities are assigned within the OU (i.e., how they are allocated among the OU's players). An organization chart setting out the OU's internal structure combined with a RACI matrix (Responsible, Accountable, Consulted, Informed)[29] can be used for this purpose.

The program charters must enable the organization to clearly identify, at a minimum and for each MCM, which OU is responsible for (1) identifying the need, (2) providing funding, (3) doing implementation/installation, (4) ensuring maintenance, (5) conducting inspections and (6) providing training on how to operate/maintain the measure. Note that these six governance elements might not be applicable to all MCM. For instance if a MCM is a process, then the governance element "providing funding" might not apply. If the governance of MCMs is well established, program charters should be complementary and, together, they should entirely cover all the activities related to proper MCM functioning (mutually exclusive and collectively exhaustive (MECE) principle).

[29] From Racichart online: https://racichart.org/

6.4.3 The MCMs governance matrix

The information derived from the program charters can be summarized in a MCMs governance matrix. In such a matrix, each row corresponds to a MCM and allows identifying which OU is responsible for each governance element shown in the column headers. A question mark indicates that it is not known who is responsible for that governance element. Obviously, the more question marks there are in a row, the weaker the governance of that MCM is, and therefore it must be strengthened. To assess each governance element related to a MCM, the following scoring system is used:

- 1 point, when the element is clearly defined;
- 0.5 points, when the element is partly (or not clearly) defined;
- 0 points, when the element is not defined;
- Non-applicable (n/a) when the element does not apply.

In addition, a General Governance Index (GGI) is calculated for each MCM. A MCM can potentially obtain a maximum GGI of 6 points out of 6, for a total of 100% (when all six governance elements apply). The following indicators are used to represent the MCMs' GGI: between 80% and 100% = green = satisfactory; between 60% and 80% = yellow = fair; less than 60% = red = inadequate. These indicators then provide the organization a general assessment of the state of governance of each MCM and enable it to target areas that require improvement. It is important to note that an MCM's GGI concerns only the distribution of roles/responsibilities among OUs in respect of that MCM. It is not intended to assess whether or not an activity related to a governance element is being executed well (e.g., if training is appropriate). That will be established when the governance of the CFR for OUs is evaluated (section 6.5).

Table 6.1 shows a partial sample MCMs governance matrix. This matrix is presented in a generic way so it can be used as a template by any organization wishing to implement the framework.

Tableau 6.1 MCMs governance matrix (partial)

MCM	OU responsible for…						MCM GGI
	Need	Funding	Implementation / Installation	Inspection	Maintenance	Training	
MCM1	OU1 and OU3	OU2	OU5	OU6 and OU7	OU7	OU8	100.0%
MCM2	OU8	n/a	OU8	?	n/a	?	50.0%
MCM3	OU1 or OU4?	OU2	OU5	OU6	OU4	?	75.0%
…	…	…	…	…	…	…	…

In this example, if we examine MCM1, the GGI for this measure is 6/6 (100%) because all six governance elements are clearly assigned to OUs. For MCM2, on the other hand, we see that OU8 has assumed responsibility for identifying the need and implementing the measure but none of the OUs has assumed responsibility for inspecting the measure or providing the training (note that funding and maintenance do not apply). Therefore, the GGI for MCM2 is 2/4 (50.0%). Thus, the governance of this MCM must be clarified to ensure one or more OUs take responsibility for inspecting the measure and ensuring appropriate training. Finally, in the case of MCM3, it seems unclear who, between OU1 and OU4 is responsible for identifying the need for this measure. In addition, it appears that no OU has taken responsibility for relevant training. Consequently, the GGI for MCM3 is 4.5/6 (75.0%) because four of the six governance elements are clearly assigned to OUs, one is not clearly assigned and one is not assigned. Thus, the governance of this MCM must be clarified as it could lead to inconsistent deployment of the measure (e.g., standardization or integration problems), as well as problems affecting its operation or maintenance (related to the necessary training). It must be noted that a more complex calculation method assigning weights to the governance elements based on their relative importance could be used. An example of such technique for weighting criteria is the combination of Analytic Hierarchy Process (AHP) and Delphi methods (Bagherigorji et al., 2022; Heydari et al., 2023; Taleai and Mansourian, 2008; Nasiri et al. 2019; Zhao et al., 2023). However, the works conducted with the partnering organization suggest that the indicators proposed in this article are quite sufficient when starting to implement an IRM governance framework. Eventually, as maturity increases, an organization could adopt a more sophisticated method. For as long as the same method is used for all MCMs to allow comparison.

The SMM aims to ensure that IRM is horizontally integrated; that is, (1) each OU (and its players) is aware of its own roles/responsibilities and those of the other OUs related to the proper

functioning of MCMs, and (2) all activities required for the smooth functioning of MCMs are assigned to OUs. These tools also add value in a context of environmental/organizational changes. Threats, assets, MCMs and players within organizations change. De facto, roles/responsibilities related to MCMs change too and become less clear as changes occur, especially in a context where systems are becoming increasingly integrated/interconnected. In this context, the goal of IRM is to ensure that these tools are maintained/updated over time so that they always reflect the organization's reality. Needless to say, ensuring that roles/responsibilities within an organization are always clearly assigned/understood is part of sound governance practice.

6.5 The CFR: Achieving the goal of strategic integration of IRM

A frame of reference is "a set of ideas or facts that a person accepts and that influences the person's behavior, opinions, or decisions"[30]. With regard to IRM, all the OUs responsible for managing ARM (and their actors) must conjunctly adhere to common principles and rules that guide their thoughts, decisions and actions, hence the expression CFR.

The CFR is intended to ensure that the organization's strategic objectives (in terms of risk management) filter down to the tactical and operational level in a logical, coherent sequence, making it possible to achieve the goal of strategically integrating risk management and decentralizing its actions toward the various organizational players. Of course, part of the CFR is established by the program charters (i.e., OUs' missions, objectives, and roles/responsibilities), but another portion must be established through a set of key elements such as policies, directives, processes, standards and key performance indicators (KPIs). Figure 6.4 illustrates the CFR structure and its elements.

[30] From Cambridge Dictionary online: https://dictionary.cambridge.org/dictionary/english/frame-of-reference.

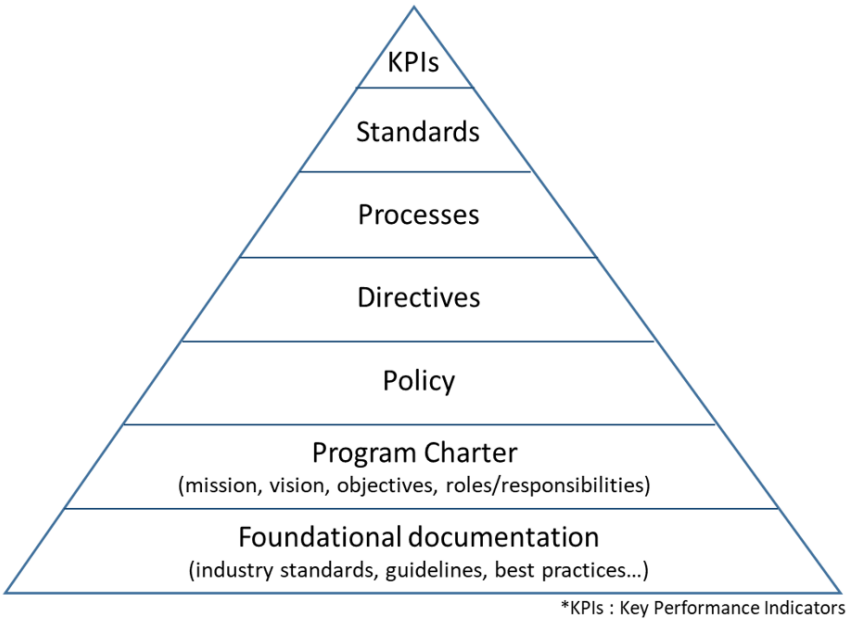


Figure 6.4 CFR structure and its elements

Thus, the second IRM-related governance indicators an organization needs concern this CFR.

6.5.1 The policies and directives

A policy is a statement regarding the purpose of an action and the preferred means of carrying it out (Canadian Encyclopedia, 2014). A directive is "an authoritative order or instrument issued by a high-level body or official"[31]. Directives specify the meaning to be given to a policy, clarifying what must or can be done and what must not or cannot be done.

With regard to the CFR, each OU must define a clear policy that stems directly from its mission and establish directives that cover all of its objectives (as stated in its policy and program charter). In terms of IRM, the key is then to ensure that the contents of the OUs' policies and directives match those in their program charters and the MCMs governance matrix (table 1). For example, if in its program charter a OU took responsibility for providing training associated with an MCM, then its directives should include a mention of this, stipulating, for instance, that all the players operating this MCM (or interfacing with it) must have taken the related training. In this case, we will also expect to find training documents available for these players and a follow-up process to validate who has successfully received/passed the training and who has not.

[31] From Merriam-Webster online: https://www.merriam-webster.com/dictionary/directive.

If the governance is well established, policies and directives should be complementary and, together, they should allow to meet all of the organization's risk management objectives/expectations. For example, for the "Physical Security" OU, whose mission consists in preventing unauthorized physical access to the organization's assets (Center for Development of Security Excellence [CDSE], 2017), the policy might mention that it covers all aspects related to site access control and monitoring. This policy might therefore refer to specific access management and surveillance directives that state, for example, that all entrance doors to facilities must be equipped with electronic access control and sites must have surveillance cameras, among other things. Meanwhile, the "Building Management" OU, whose mission is to ensure that all systems related to the built environment function correctly (International Facility Management Association [IFMA], 2024), must ensure that its directives that concern maintenance include statements regarding the maintenance of the access control and monitoring systems. These directives might then refer to specific maintenance processes/standards for these MCMs that come from their suppliers/manufacturers.

6.5.2 The processes

A process is "a series of actions or operations conducing to an end"[32]. Processes support directives by establishing the steps to be taken to achieve a goal/deliverable.

With regard to the CFR, each OU must document the main processes that enable it to achieve its objectives, as established in its program charter and supported by its policy and directives. Processes must make it possible to standardize approaches/methods within each OU and within the organization, and also refocus players' roles/responsibilities in relation to risk management. Since processes are made up of tasks, which are assigned to different players, it becomes possible to identify which players are associated with which risks and thereby achieve the decentralization of risk management that IRM strives for (IRGC, 2017; Morabito and Robert, 2023b). For example, the directive regarding access management (mentioned previously) could refer to a visitors' management process that sets out the steps to be taken in authorizing a visitor to access one of the organization's facility. In this process, the receptionist will have specific tasks to execute in order to check the visitor in (e.g., verify their identity, have them sign the visitors' register, and give them

[32] From Merriam-Webster online: https://www.merriam-webster.com/dictionary/process.

a visitor pass); the host will also have specific tasks related to accompanying the visitor (e.g., inform them of evacuation procedures, accompany them throughout the visit, and escort them outside when the visit is over). The visitors' management process therefore associates two players (receptionist and host) with the risk of unauthorized access by a visitor. If for any reason this process is not followed, the risk increases that an unauthorized person will access a facility (or an area within a facility) that they should not be able to access. This increased risk of unauthorized access (OU: Physical Security) brings other risks with it such as the risk of accident/injury (OU: Health and Safety), the risk of compromising confidential information (OU: Information Security), or the risk of a human error interrupting operations (OU: Business Continuity). Thus, particular attention must be paid to processes that involve several OUs since they may create confusion regarding the sharing of roles/responsibilities, which can be a potential source of risks. This is why it is important to have a crosscutting view of risks – which is precisely what IRM allows. Moreover, since processes are not necessarily fail-safe, it is important to analyze them in order to identify any inherent potential vulnerabilities (failure points) within these processes that could result in additional risks for the organization. Business Process Analysis tools may contribute to developing robust, effective processes[33].

6.5.3 The standards

Standards are meant to ensure the quality of a product/service or the compliance of an action. They are based on best practices established by recognized organizations, and fine-tuned through consensus among experts in the relevant domains; they are normally formulated to minimize risks or potential accidents (ISO, 2023a).

With regard to the CFR, standards support directives and processes by establishing how things should be done. To this end, each OU must identify the main standards related to the MCMs that have been deployed and are associated with its sphere of competence. For example, the directive regarding access management (mentioned previously) might state that employees' access cards must comply with the "Physical Security" OU's applicable standard; this standard could specify the size and characteristics of the access card and photo, for example. However, other OUs might also have requirements applicable to access cards that must be met. For example, the "Information

[33] From IBM: https://www.ibm.com/blog/business-process-analysis/.

Security" OU might stipulate that the card must not disclose any personal information about its holder, while the "Computer Security" OU might insist that communication between the access card and the control server must be end-to-end encrypted.

Standards can also be used to assess MCMs' compliance by providing a basis for comparison between the observed and recommended states for these MCMs. For example, a fire protection system in an old building might not respect a standard/regulation now in force. Another MCM might be in a state of advanced deterioration such that it can no longer appropriately fulfill its function. This information should be reflected in the aggregation model (e.g., by using a specific indicator) to show that these MCMs are non-compliant and represent vulnerable points for the organization. IRM should ensure that all standards applicable to MCMs are known and respected but also that they are periodically updated, because standards change with time and may also vary from one region to another (depending on legislation).

6.5.4 The key performance indicators (KPIs)

KPIs are metrics that show the progress made toward achieving specified objectives[34]. The management of large organizations depends crucially on these indicators (Drucker, 1954) since they allow them to prioritize their actions and measure these actions' effects on performance by means of periodic reporting (scorecards) (Dolence and Norris, 1994; Kaplan and Norton, 1996). It is therefore important to define these indicators appropriately. It is recommended that SMART (Specific, Measurable, Assignable, Realistic and Time-related) indicators be used for this purpose (Doran, 1981). Needless to say, reporting is part of sound governance practice since it makes it possible to ensure that KPIs are followed up periodically.

With regard to the CFR, each OU is responsible for defining the KPIs that are best aligned with its objectives and monitoring its progress in achieving them. These KPIs must allow the organization's top management to assess the OUs' performance or the status of any other relevant element that may be reported on (Kaplan and Norton, 1996) (e.g., policy, directives, processes, standards, MCMs' state). They must enable the organization to detect any gaps between an objective to be achieved (hoped-for ideal) and the situation on the ground and to identify actions to be taken to fill these gaps.

[34] From KPI.org: https://www.kpi.org/KPI-Basics/.

6.5.5 The OUs governance matrix

The information derived from the CFR should be summarized in an OUs governance matrix wherein each row corresponds to an element from the CFR and each column corresponds to an OU; the last column concerns IRM. To assess each element of the CFR, the same scoring system as in section 2.3 is used. However, to make this example slightly different and to illustrate how a weighted approach can be used, we have taken into consideration that the elements of the CFR don't have the same importance (weighting). For the purposes of this article, the weighting was determined arbitrarily. However, here again, an organization could use a more elaborated technique for weighting the various criteria.

To represent the OUs' GGI, the same indicators as used in the MCM governance apply. However, in addition to assessing the governance of each OU, the organization also needs to assess how integrated the elements of the CFR are. To do this, a GGI is calculated for IRM (which represents the organizational standpoint). To calculate this indicator, the total number of points that an element of the CFR gets is multiplied by the "mutual awareness and complementarity" factor (MAC factor). This factor is determined as follow:

- 1 point, when the element is shared among OUs and complementary;
- 0.5 points, when the element is partly shared among OUs and complementary;
- 0 points, when the element is not shared among OUs and complementary.

Table 6.2 shows a sample OUs governance matrix. Here again, the matrix is presented in a generic way so it can be used as a template by any organization wishing to implement the framework.

Tableau 6.2 OUs governance matrix

CFR elements	Weight	OU1	OU2	OU3	OU4	OU5	OU6	OU7	OU8	Total score (/8)	MAC factor	IRM
Mission	**10%**	1	1	1	1	1	1	1	1	8	1	1
Objectives	**15%**	1	0.5	1	1	1	1	1	0.5	7	1	0.9
Roles/responsibilities	**15%**	1	0.5	1	0.5	1	1	1	0.5	6.5	0.5	0.4
Policy	**10%**	1	1	1	1	1	1	1	1	8	0.5	0.5
Directives	**15%**	1	0.5	1	0.5	1	1	1	0.5	6.5	0.5	0.4
Processes	**15%**	1	0.5	0.5	0.5	1	0.5	1	0.5	5.5	0.5	0.3
Standards	**10%**	0.5	0.5	0	0	1	0	0	0	2	0	0
KPI	**10%**	0.5	0.5	0	0	0.5	0	0	0	1.5	0	0
OU GGI (%)		**90.0**	**60.0**	**72.5**	**57.5**	**95.0**	**72.5**	**80.0**	**50.0**			**45.5**

In this example, if we consider the "Mission" element, we see that each OU has obtained 1 point, for a total of 8/8 points. This means each OU has clearly defined its mission. Because the MAC

factor is 1, this means that the mission statement are shared among OUs (so every OU is aware of the other OUs' missions) and they are complementary (so to achieve all of the organizational strategic objectives set for risk management). In terms of IRM, the organization therefore obtained 1 point (8/8 x 1). On the other hand, when we consider the "Processes" element, we see that only OU1, OU5 and OU7 have fully documented their main processes, whereas the other OUs have only partly documented them. The total points for the OUs is therefore 5.5/8. Because the MAC factor is 0.5, this means that the processes are partly shared among OUs and complementary. In terms of IRM, the organization therefore obtained 0.3 points (5.5/8 x 0.5). Working in the other direction, if we consider OU1, we can see that it has clearly defined its mission, objectives, roles/responsibilities, policy, directives and processes but it has only partially documented its standards and KPIs. Its overall GGI score, based on the weighting assigned to each element of the CFR, is therefore 90.0%. If we rely on these indicators alone, we could state that, overall, OU5 has the highest governance status (GGI of 95.0%), while OU8 has the poorest (GGI of 50.0%). From an IRM standpoint, the organization achieved a GGI of 45.5%.

Ultimately, the purpose of this matrix is to provide simple indicators of the state of governance in relation to the CFR that are relevant and representative of reality, can be monitored periodically, and allow the organization to clearly identify the areas that need improvement. Thus, these indicators kind of provide a brief assessment of each OU's level of maturity in respect of risk management and of the organization's in respect of IRM. That said, the indicators' purpose is not to provide a comprehensive assessment of the OUs' maturity. Governance maturity is a relatively recent concept, but in general, it tends to indicate how well defined an organization's governance is (Institute of Internal Auditors [IIA], 2022). The works with the partnering organization show that for an organization that is only starting to implement an IRM governance framework, the indicators proposed in this article are quite sufficient. Then, as its maturity increases, the organization may opt for a more comprehensive organizational maturity assessment model such as the IIA's Maturity Model for Governance (IIA, 2022) or the ISO37004 standard (ISO, 2023b) which cover an organization's governance as a whole and not just IRM-related governance.

6.6 The overall representation of IRM-related governance

The GGIs for the MCMs (table 1) and OUs (table 2) can be introduced into the aggregation model to obtain an overall representation of the status of the organization IRM-related governance and identify where weaknesses reside. Figure 6.5 illustrates this result.

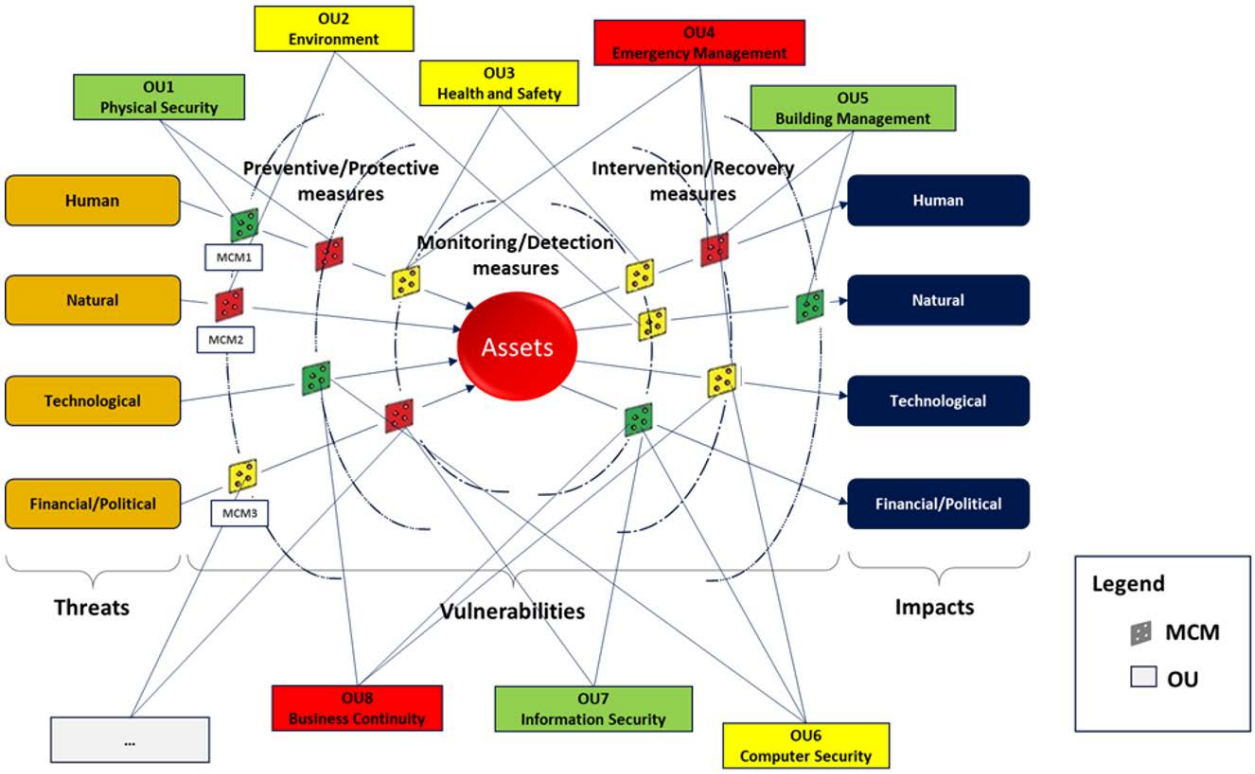


Figure 6.5 Overall representation of the status of the organization IRM-related governance

In this representation, each MCM is shown in the color that corresponds to the result it obtained in its GGI (table 1) and is positioned at the appropriate location, depending on whether it applies to prevention/protection, detection/monitoring, or intervention/recovery. We can therefore pick out MCM1, MCM2 and MCM3 in the model, along with all the other MCMs. Note that a single MCM might be placed in more than one place if it has several functions. Similarly, each OU is represented in the color corresponding to the result it obtained in its GGI (table 2). At the center of the model, the organization (which is represented through its assets) is also represented in the color corresponding to the result it obtained in its GGI (table 2, column IRM). Indicators shown in red should obviously represent a red flag and should lead to a more in-depth analysis of what led to these results and an action plan to remediate the situation.

Other simple IRM-related governance indicators can also be derived from the illustration. For example:

1. of the 8 OUs, 3 (37.5%) have satisfactory governance, 3 (37.5%) have fair governance, and 2 have inadequate governance (25.0%);
2. of the 13 MCMs, 4 (30.8%) have satisfactory governance, 5 (38.4%) have fair governance, and 4 have inadequate governance (30.8%);

These indicators, along with the ones in table 1 and table 2, can be track periodically to assess the evolution of the organization's IRM-related governance.

In addition to these simple analyses, figure 6.5 allows users to identify the paths of least resistance (in terms of governance) along which failures could propagate. Thus, we note that the following four paths present governance weaknesses that make them more subject to the propagation of failures:

1. the Natural threats – Assets – Human impacts path;
2. the Natural threats – Assets – Technological impacts path;
3. the Financial/political threats – Assets – Human impacts path;
4. the Financial/political threats – Assets – Technological impacts path.

Naturally, several other kinds of analyses would be possible and our goal here is simply to illustrate some. Overall, though, if an organization manages to improve its IRM-related governance, it will make enormous gains, which will be reflected in gains for the management of the majority of the risks it faces.

6.7 Discussion and conclusion

This article presented an IRM governance framework dedicated to large organizations, which was developed on the basis of empirical work carried out in a large Canadian organization. Resting on two pillars (a SMM and a CFR), this framework aims to ensure that all activities conducted by the various OUs responsible for managing ARM are coordinated, concerted and focused towards achieving a common objective.

Although this framework was designed to be easy to use, some limitations make its implementation in an organization face certain challenges. First, it requires the organization to engage in a process of change of its organizational culture shifting from a siloed/vertical approach to managing risks towards a more collective/crosscutting one. Yet, change management requires addressing certain challenges of its own that haven't been addressed in this article. A first challenge consists in convincing all stakeholders of the need to change. Then, to actually engage in the process of change, they must dedicate the appropriate resources. Since IRM is a long term initiative, it is highly recommended that a dedicated entity within the organization be given the mandate to do so. This entity can then guide the organization and its OUs through change and ensure risk management is fully integrated and generates valuable outcomes.

To this end, a certain level of competence/expertise in risk management is required. Hence, a second challenge is to identify the right players to be part of this entity. In the context of this article, the organization has benefitted from the expertise of the researchers (the authors), however, it would be advantageous to identify more rigorously what kind of profile (in terms of education, competencies and skills) these players should have. This could also help identify if a specific training is required prior to implementing the framework. To validate this point, it would be necessary to conduct a project with a few other large organizations that would be willing to implement the framework with less external intervention. This could also help validate that the framework can be easily adapted to other large organizations, confirm its pragmatism/effectiveness and, in the end, contribute to improving it.

A third challenge resides in how such entity can be fitted within the organizational structure. This article hasn't addressed this issue. Nonetheless, the work conducted within the partnering organization have shown that a cooperative structure allowing to consolidate the crosscutting and strategic integration of risk management is necessary. This structure is needed to correlate all the information coming from the various OUs and to facilitate the horizontal and vertical transfer of information between the OUs and between the organizational levels. More work is therefore needed to define the shape that this structure ought to take and to determine how it can be harmoniously fitted into the organization's functional structure.

Finally, another challenge concerns the technical aspect of IRM. Indeed, the value that IRM adds to organizations is not only based on its governance aspect, but also on its capacity to generate

KRIs that could not be created without the aggregation of risk-related information from all its OUs. Thus, while in this article the aggregation model has been used to address the governance aspect of IRM, it must also be used to address the technical aspect of IRM, that is from the perspective of risk analysis/assessment. More work is therefore necessary to develop indicators capable of representing the three parameters of risk (i.e., threats, vulnerabilities and impacts) and determine how these must be aggregated/correlated to provide value-add KRIs. Regarding this last point, it would be interesting to analyze how this framework can deal with new, emerging risks characterized by more ambiguity, uncertainty and complexity and for which these parameters are not so easily determined. Answering these questions would ensure the framework can evolve over time so to always remain relevant, and demonstrate the need for organizations to transition to IRM so they can be in a better position to face these new, emerging risks.

CHAPITRE 7 ARTICLE 4 : A COOPERATIVE STRUCTURE FOR INTEGRATED RISK MANAGEMENT IN LARGE ORGANIZATIONS

Morabito, L. et Robert, B. (). 'A cooperative structure for integrated risk management in large organizations', *Int. J. Decision Sciences, Risk and Management*, Soumis pour publication le 6 juin 2025.

7.1 Mise en contexte et présentation de l'article

Les travaux effectués dans le cadre du chapitre précédent arrivent à la conclusion que pour consolider les intégrations transversale et stratégique de la GIR, une structure de coopération est requise. Cette structure de coopération doit permettre de faciliter et de formaliser les échanges d'informations et de connaissances entre les différentes UF responsables des AGR ainsi qu'entre les niveaux opérationnel, tactique et stratégique de l'organisation.

Ainsi, en lien avec le deuxième objectif spécifique de ces travaux de recherche (et deuxième composante d'un EC), l'objectif de ce chapitre est de définir cette structure de coopération. Celle-ci devra pouvoir s'intégrer à la structure fonctionnelle des grandes organisations. En effet, cette dernière est bien adaptée aux opérations courantes. L'objectif n'est donc pas de la modifier, mais plutôt de faire en sorte que la structure de coopération mise sur pied pour la GIR puisse s'y intégrer harmonieusement. Pour y parvenir, il faut donc (1) déterminer la forme (et le fonctionnement) de cette structure de coopération et (2) déterminer comment cette structure doit s'arrimer à la structure fonctionnelle.

Concernant la forme de la structure de coopération, les travaux avec l'organisation partenaire ont clairement établi le besoin pour la mise sur pied d'une Équipe dédiée à la GIR (ÉGIR). Cette équipe, multidisciplinaire et transversale, doit s'établir au niveau tactique. En effet, l'arrimage entre les niveaux opérationnel et stratégique de l'organisation ne peut se faire qu'à ce niveau, puisqu'il y existe une bonne compréhension des objectifs stratégiques que la haute direction cherche à atteindre ainsi qu'une bonne compréhension des enjeux opérationnels. Pour cela, la structure de coopération qui a été élaborée avec l'organisation partenaire, et qui est recommandée dans cette thèse, est illustrée à la figure 7.1. Cette structure s'inspire du modèle des Trois Lignes De Défense

(3LDD) de l'*Institute of Internal Auditors* (IIA) (IIA, 2020) et intègre le concept d'Unité d'Efforts (UE) (Greco, 1995 ; Kingsley, 2017a ; United States Department of Defense [US DOD] ; Wilder, 2012).

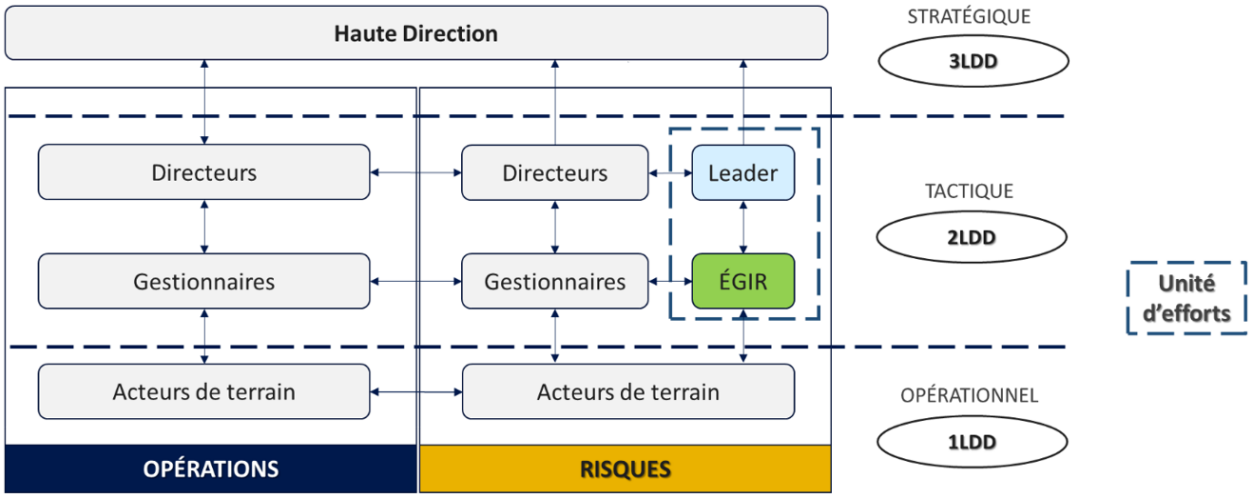


Figure 7.1 Structure de coopération suggérée pour la GIR

Comme le montre cette figure, cette structure propose, dans un premier temps, de scinder les activités organisationnelles en deux grands vases communicants, l'un lié à la gestion des opérations et l'autre lié à la gestion des risques. Dans l'organisation partenaire, cette division existait déjà. Ensuite, la structure propose d'accoler à chaque niveau organisationnel (opérationnel, tactique et stratégique) une étiquette correspondant à une ligne de défense du modèle des 3LDD. Finalement, du côté des risques, la structure prévoit de positionner une UE responsable de la GIR en parallèle des AGR et, comme mentionné plus tôt, au niveau tactique (donc, au niveau de la 2LDD). Dans cette structure, tout le volet relié aux activités courantes des UF responsables des AGR suit donc son cours normal, mais tout un volet parallèle dédié à la GIR, donc dédié à l'intégration (agrégation et corrélation) de tous les extrants produits par les UF responsables des AGR, vient s'ajouter à la structure.

Concernant l'arrimage de la structure de coopération à la structure organisationnelle, trois options ont été analysées :

1) l'arrimage selon une structuration fonctionnelle ;
2) l'arrimage selon une structuration matricielle ;
3) l'arrimage selon une structuration agile et organique.

L'arrimage selon une structuration fonctionnelle est une première façon d'arrimer l'ÉGIR à la structure organisationnelle. Dans cette façon de faire, l'ÉGIR relève d'un leader compétent et est positionnée verticalement aux autres UF responsables des AGR. La figure 7.2 illustre cette structuration.

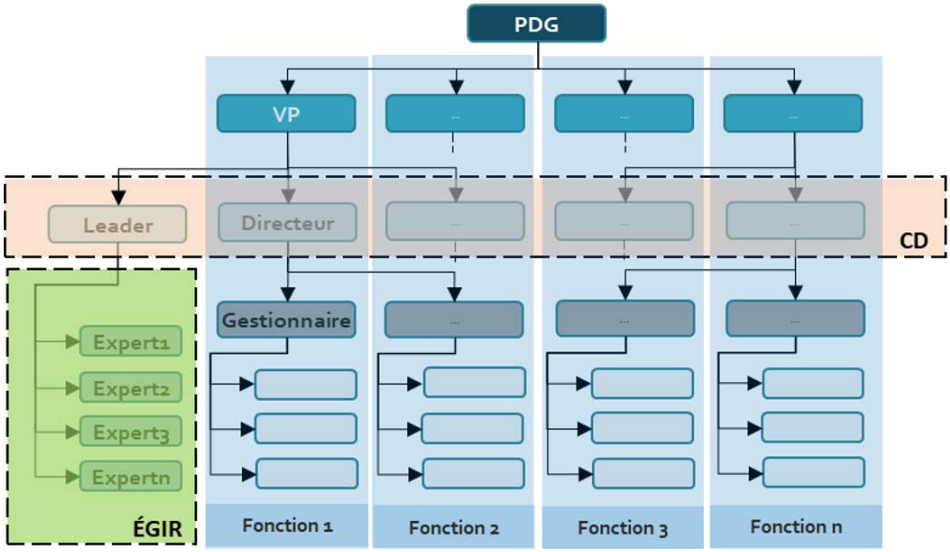


Figure 7.2 Arrimage de la structure de coopération selon un mode de gestion fonctionnel

L'avantage évident de cet arrimage est qu'il ne vient pas déstabiliser la structure organisationnelle fonctionnelle puisqu'il ne la change pas. Cependant, cette structuration ne résout pas d'emblée l'enjeu de la transversalité puisque les membres de l'ÉGIR n'ont pas de liens d'attache formels avec les autres UF responsables des AGR (fonctions 1, 2, 3 et suivantes). Sur le long terme, cet arrimage risque de cloisonner la GIR et pourrait finir par amplifier le problème qu'elle tente de résoudre en créant des tensions entre les experts de l'ÉGIR et les experts des UF responsables des AGR. Ces tensions pourraient créer des barrières au niveau des échanges d'informations entre ces UF et l'ÉGIR : chacun voulant conserver la chasse gardée sur ses informations, ses décisions et ses actions.

L'arrimage selon une structuration matricielle est une deuxième façon d'arrimer l'ÉGIR à la structure organisationnelle. Largement employée dans le domaine de la gestion de projets, cette structure possède l'avantage de pouvoir faire travailler ensemble des acteurs possédant des expertises différentes (donc, provenant de plusieurs silos organisationnels différents) tout en permettant que les actions spécifiques à une discipline donnée soient décentralisées vers celle-ci (Jacob et Michel 2020). Ce point est intéressant puisque, comme il l'a été expliqué lors de la revue

de la littérature, cette décentralisation vers les acteurs est une caractéristique importante de la GIR. Ainsi, dans une telle structure, les personnes sélectionnées pour faire partie de l'ÉGIR demeurent aussi membres à part entière de leur UF originelle. Elles sont alors beaucoup mieux placées pour jouer pleinement leur rôle de pivot entre l'ÉGIR et les UF responsables des AGR, permettant ainsi un accès direct aux informations des UF en plus de constituer une voie de rétroaction directe pour les résultats issus des travaux de l'ÉGIR vers celles-ci. La figure 7.3 illustre cette possibilité.

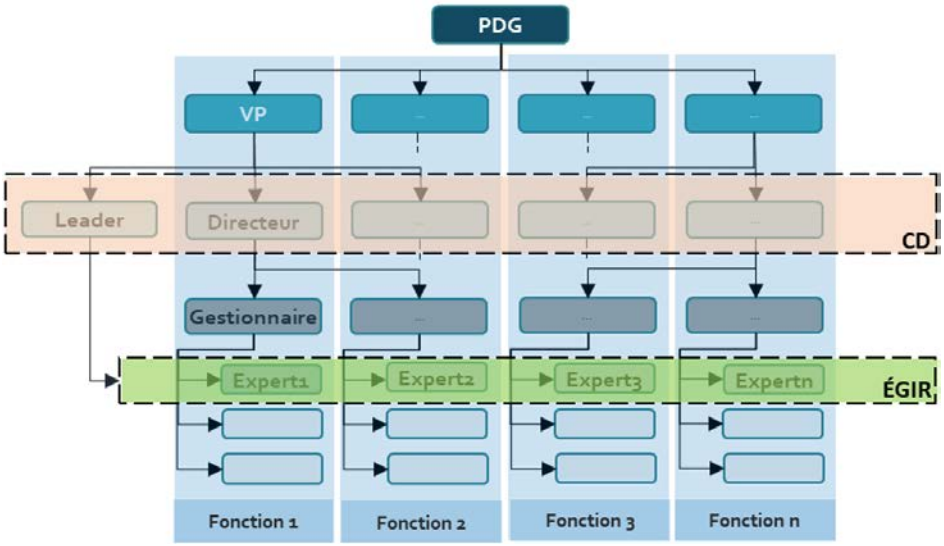


Figure 7.3 Arrimage de la structure de coopération selon un mode de gestion matriciel

Néanmoins, dans ce mode de gestion, les membres de l'ÉGIR se retrouvent alors à combiner principalement deux fonctions et se rapportent aussi à deux autorités différentes (le leader de l'ÉGIR et le gestionnaire de fonction) si bien qu'il peut en résulter des situations conflictuelles au niveau de la priorisation des tâches à effectuer (Jacob et Michel 2020). Si cela peut fonctionner dans le cadre de projets dont la durée est déterminée, il en est autrement dans le contexte d'initiatives pérennes comme la GIR. En effet, le manque de temps est un obstacle majeur au déploiement, au rendement et à la pérennité d'une collaboration (Morabito et Robert, 2023a) et il pourrait devenir contre-productif que les personnes qui participent à une tâche aussi complexe que la GIR aient à réaliser d'autres tâches en parallèle. Ainsi, cette structure pourrait créer un épuisement sur le long terme des membres de l'ÉGIR qui ferait en sorte qu'il deviendrait très difficile de maintenir l'intérêt au-delà d'un certain temps. Or, le maintien de l'intérêt est un autre enjeu de taille au maintien d'une collaboration sur le long terme (Morabito et Robert, 2023a). Il serait donc souhaitable que les personnes qui feront partie de l'ÉGIR soient dédiées à cette

problématique, tout en s'assurant qu'elles demeurent membres à part entière des UF desquelles elles sont issues[35].

L'arrimage selon une structuration de type agile et organique est une troisième façon d'arrimer l'ÉGIR à la structure organisationnelle. Ce mode de gestion est tout indiqué pour les initiatives qui intègrent le travail en mode collaboratif, l'intégration transversale et l'ouverture vers les partenariats (Jacob et Michel, 2020). Un intérêt de la structuration en mode agile et organique tient du fait que l'ÉGIR peut être modulée (au sens du nombre et de l'identité des acteurs qui y participent) en fonction de la problématique de risque analysée. Le fonctionnement de l'ÉGIR est donc beaucoup plus « malléable et flexible » permettant ainsi d'exploiter l'ensemble des connaissances individuelles disponibles dans l'organisation en faisant intervenir les bonnes personnes au bon moment. La figure 7.4 illustre cette possibilité.

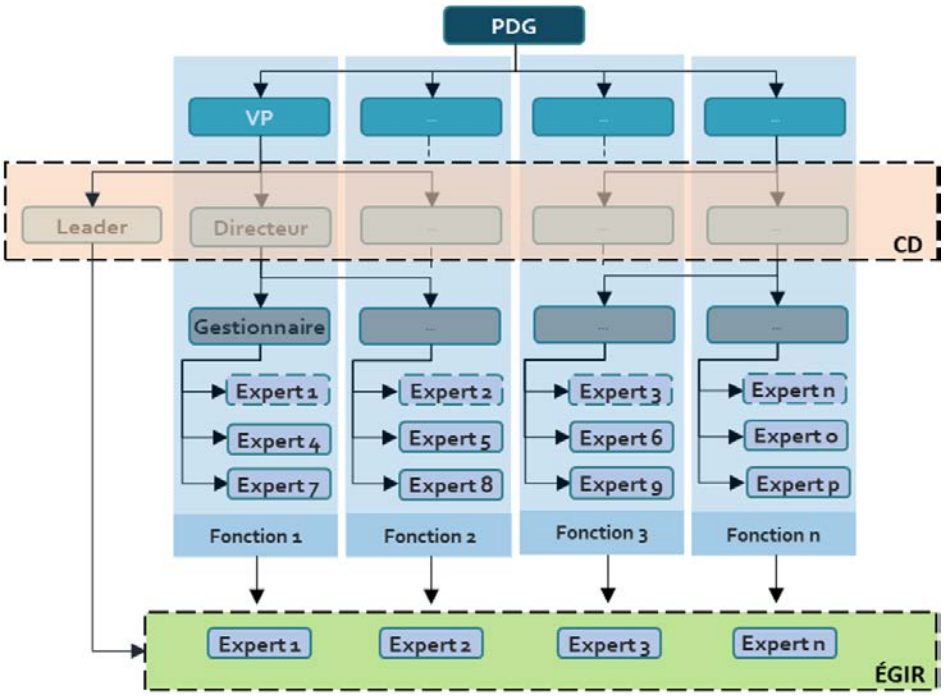


Figure 7.4 Arrimage de la structure de coopération selon un mode de gestion agile et organique

[35] Dans le cadre des travaux avec l'organisation partenaire, une structure matricielle (de type faible) avait été mise en place. Cette structure permettait d'avoir une représentation de toutes les UF participantes au niveau de l'équipe de projet et était parfaitement adaptée au contexte d'un projet de recherche temporaire. Néanmoins, en combinant leurs tâches habituelles et leurs tâches liées à la GIR, la charge de travail sur les membres de l'équipe de projet était trop importante, créant une situation dans laquelle les activités quotidiennes de ces experts prenaient toujours le dessus sur le projet de recherche et qu'au bout du compte, ces personnes devaient consacrer des heures supplémentaires pour répondre aux besoins de ce projet, générant ainsi un certain épuisement chez ces ressources. Cette structure ne serait donc pas envisageable dans un contexte où l'on vise à pérenniser la GIR. Pour que cela fonctionne de manière efficace, l'équipe mise sur pied pour la GIR doit être entièrement dédiée à cette problématique.

L'un des avantages de la structuration en mode agile et organique est lié à la liberté d'action et de réflexion qui vient avec cette forme de structure (Jacob et Michel, 2020). Cette liberté d'action est d'ailleurs souhaitable (voire, requise dans une initiative comme la GIR) afin d'assurer l'indépendance entre les fonctions opérationnelles de l'organisation et les fonctions de gestion des risques (IIA, 2020). Cependant, l'alternance au niveau des membres de l'ÉGIR en fonction de la problématique de risque analysée pourrait nuire au maintien de la vision commune sur les objectifs à atteindre et sur la capacité pour ces acteurs à développer leur ISP. Ainsi, il serait plus opportun, pour favoriser la consolidation des liens interpersonnels (lien de confiance) et maintenir la vision unique sur les objectifs à atteindre, qu'un noyau stable de membres de l'ÉGIR demeure constant et que ceux-ci fassent intervenir, au besoin, des personnes externes à l'ÉGIR lorsque des compétences ou des connaissances particulières sont requises pour certaines analyses. Dans ce contexte, l'arrimage de la structure de coopération à la structure fonctionnelle se voudrait un hybride entre la structuration matricielle (forte) et la structuration agile et organique. La figure 7.5 illustre ce cas.

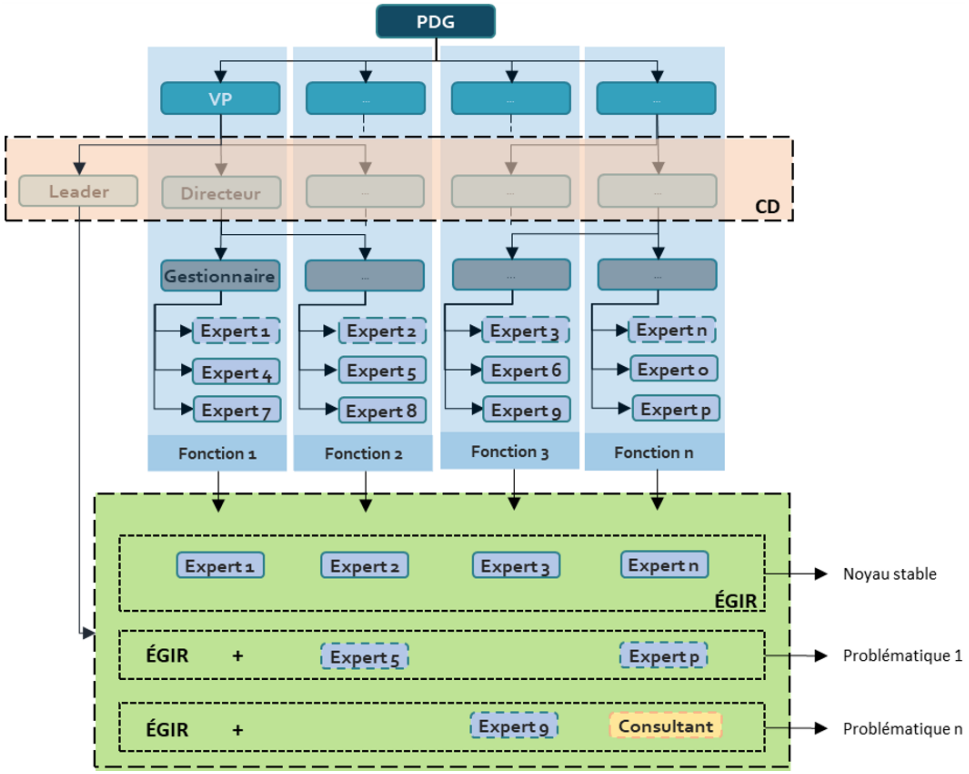


Figure 7.5 Arrimage de la structure de coopération selon un mode de gestion hybride (matricielle forte et agile et organique)

L'article ci-après présente ainsi la structure de coopération pour la GIR proposée dans cette thèse. Le fonctionnement de cette structure est représenté à la figure 7.1 et son arrimage à la structure organisationnelle s'apparente à un mode de gestion hybride combinant un mode de gestion de type matriciel (fort) et un mode de gestion type agile et organique, comme le montre la figure 7.5. Dans ce contexte, l'arrimage recommandé possède les mêmes avantages que la structure matricielle, sans les inconvénients liés au dédoublement de fonctions.

Finalement, l'article conclut que pour être réellement efficace, cette structure de coopération doit être mise en place dans un cadre plus large de gouvernance pour la GIR qui demande non seulement la mise en place d'un référentiel commun pour les acteurs faisant partie de l'ÉGIR (faisant ainsi référence aux travaux réalisés au chapitre 6), mais qui puisse également créer de la valeur en permettant que les ICII sur les risques qui sont réparties dans l'organisation soient agrégées en un tout cohérent fournissant des connaissances collectives nouvelles et transversales qui pourront la guider dans ses prises de décisions plus tactiques et stratégiques en regard de la gestion des risques (faisant ainsi le lien avec les travaux qui seront présentés au chapitre 8).

7.2 Abstract

Integrated Risk Management (IRM) is a crucial element of large organizations' management and decision-making. However, in large organizations, risk management is most often under the responsibility of multiple Organizational Units (OUs), each being accountable for managing an Activity related to Risk Management (ARM), such as business continuity, emergency management and physical security. Consequently, risk-related information is distributed throughout the organization, without necessary being aggregated within a common repository which can negatively impact decision-making. In this context, the functional structure of large organizations represents an issue for IRM that must be solved.

This article proposes a cooperative structure for IRM that is adapted to large organizations. Established on the basis of work done within a large Canadian organization and inspired by the Institute of Internal Auditors' three lines of defense model and the concept of unity of effort, this structure centralizes IRM-related activities within a dedicated team but decentralizes actions to all organizational players.

Keywords: cooperative structure; functional structure; governance; integrated risk management; three lines of defense; unity of effort.

7.3 Introduction

Large organizations operate in extremely volatile environments that are characterized by numerous major changes, including climatic, technological and social changes. This situation emphasizes the need for organizations to protect their assets against the threats to which they are exposed and develop their adaptability and resilience. In this context, large organizations need a more general picture of the threats they face and their vulnerability so they can determine which ones present risks that must be addressed first. This is precisely the goal of IRM: provide the organization with a more holistic view of the risks it faces to help with decision-making at all levels (operational, tactical and strategic) and ensure the cooperation and coordination of all organizational players involved in risk management (Government of Canada, 2016).

As its name indicates, IRM is intended to integrate all ARM under a single governance framework. To do this, IRM requires all organizational players who have a role in risk management to work together, in a coordinated, synergistic way, to (1) clarify their needs, priorities, roles and responsibilities towards risk management; (2) pool the information needed to identify and understand risks; and (3) ensure the coherence of the decisions and actions taken to mitigate risks (Amansou, 2019; Salim et al., 2021).

In this context, the functional structure of large organizations represents an issue for IRM since information on risks is most often dispersed throughout the organization, among several OUs operating in silos, without any true aggregation within a common repository. Decision-making regarding the actions required to mitigate risks is also dispersed among these OUs; there is rarely a single entity responsible for ensuring that these actions are coordinated and coherent (Morabito and Robert, 2025).

This article addresses this problem directly. First, it shows how the structure of large organizations represents an issue for IRM. Then, it proposes a cooperative structure for IRM that is based on the Institute of Internal Auditors' (IAA) three lines of defense (3LoD) model and the concept of unity of effort (UE).

7.4 The functional structure of large organizations: An issue for IRM

Large organizations, whether private or public, are mainly structured according to function, that is to say, in silos corresponding to a number of OUs. Although this structure is very well adapted to ongoing operations, the key issue stems from the fact that OUs usually communicate very little with each other; when communication does occur, it is generally not very formalized (Jean-Jules and Vicente, 2020; Jacob and Michel, 2020; Sarker et al., 2016). Thus, the functional structure is not very effective for addressing crosscutting problems within the organization, namely those that require a general approach (or response) that is planned by the entire organization and not by a single OU (Jean-Jules and Vicente, 2020; Jacob and Michel, 2020; Bharosa et al., 2010).

ARM in large organizations are also generally organized according to function (Jean-Jules and Vicente, 2020; Sarker et al., 2016). ARM, such as business continuity, emergency management, physical security, computer security and occupational health and safety, amongst other, are generally conducted independently (Chen et al., 2013) and are executed by various OUs. These activities are also generally carried out independently of activities that are directly related to daily operations. Consequently, risk-related information is dispersed throughout the organization, and the actions needed to deal with risks are set out in multiple plans; Decision-making regarding these actions is also dispersed throughout the organization. However, there is rarely an entity responsible for ensuring that all this information is aggregated within a common repository, nor for ensuring coherence and cohesion among all the plans and their related actions (Jean-Jules and Vicente, 2020; Bohnert et al., 2019). A situation therefore exists in which each OU, based on its roles and responsibilities, has a view of part of the system, but no OU has an overview of the entire system or the mandate to provide the organization such an overview. Figure 7.6, from Morabito and Robert (2025), depicts this situation and illustrates the risk management ecosystem in large organizations.

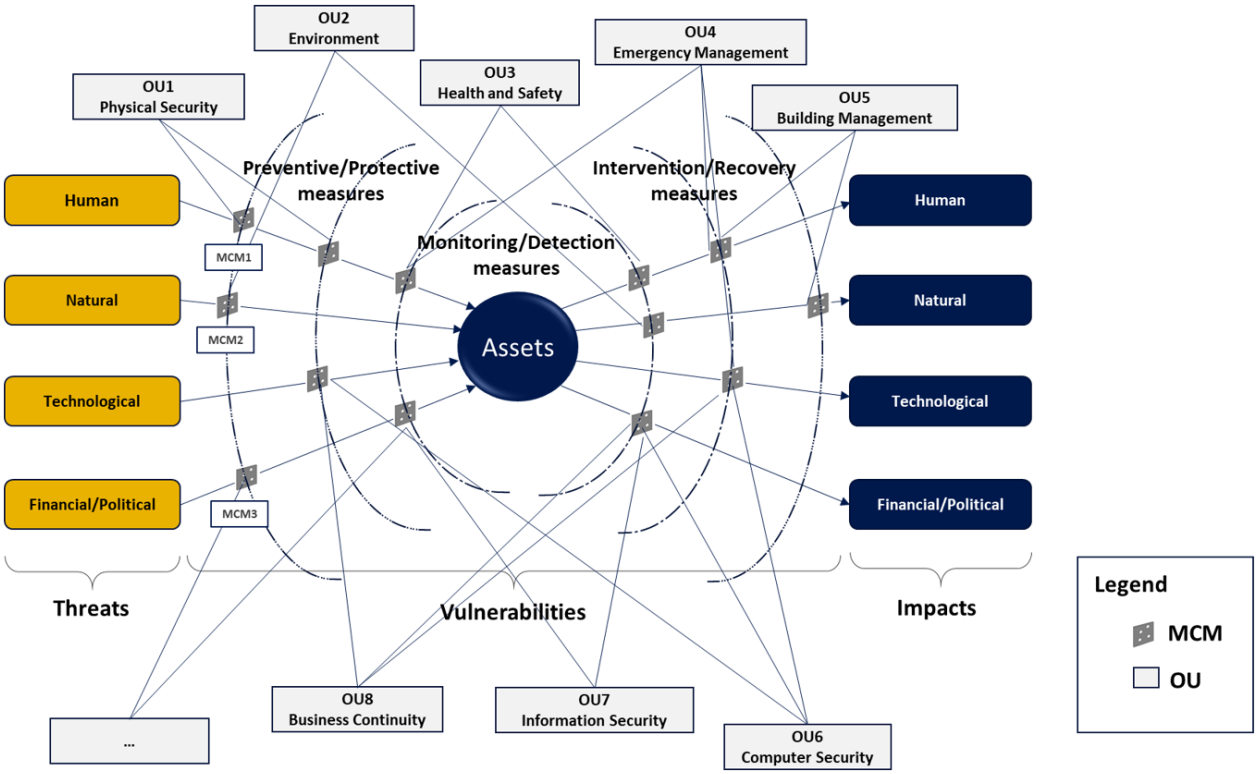


Figure 7.6 Overview of the roles/responsibilities related to ORM

This figure shows threats on the left side, the organization's assets in the center, and the impacts related to the failure of these assets at right. On both sides of the assets, we see the Mitigation and Control Measures (MCMs) implemented to mitigate risks. These MCMs may be used for prevention/protection (to prevent risky situations or protect assets from threats in the environment), detection/monitoring (to monitor the environment and detect any situation likely to affect assets), or intervention/recovery (to reduce the impacts of a disruptive event or return to normal functioning after a failure). This figure also illustrates, conceptually, the distribution of roles and responsibilities among the OUs responsible for managing ARM and for ensuring the proper functioning of MCMs. For example, if we consider OU1, Physical security, this OU is primarily responsible for protecting the organization's assets against human-type threats, and more specifically, to prevent unauthorized physical access to assets through the use of various MCMs (such as access control, alarms, cameras, security guards, etc.). However, other OUs could also have a role to play in ensuring that these MCMs function well, for example by doing maintenance or offering the necessary training to the employees who will have to operate these measures. Thus,

as figure 7.6 shows, cooperation and coordination among all these OUs is absolutely necessary to really understand the risks the organization faces and to deal with disruptive events that may affect the organization's assets.

Typically, in this kind of situation, the organization will set up a multifunctional management cell (or crisis cell), composed of representatives from all the OUs concerned, to coordinate the necessary actions to manage the disruptive events (Tena-Chollet et al., 2017). However, such cells are ephemeral by their nature. They are set up during emergencies but they are not designed to operate continuously, which presents serious limitations since managing a largescale disruptive event demands significant teamwork (Tena-Chollet, 2012). And, as in all teamwork, to ensure that the response is effective and coherent, the players must be used to working together. To this end, they must have opportunities to get together regularly so that they know and understand each other roles and responsibilities and can develop mutual trust (Hwang and Yoon, 2020; Seppänen et al., 2013) and, above all, shared situational awareness (SSA) (Tena-Chollet et al., 2017; Micouleau and Robert, 2021).

For individuals, situational awareness is the faculty whereby they become aware of their environment through all the stimuli their senses deliver to them (perception); translate them into something intelligible based on their knowledge, skills and past experiences (representation); and anticipate events likely to occur (projection) in order to take action; that is, make a decision and act based on the situation/context (Endsley, 1988; Endsley, 1995; Endsley, 2015). Perception, representation and projection are the three actions included in situational awareness at an individual's level. If several individuals are involved, we speak of SSA.

SSA enables players to construct a shared mental model (shared understanding) of a risky situation but also to establish a common operational framework that will allow them to adopt a concerted, coordinated response based on the situation/context (Chionis et al., 2022) – what is also called a common operational picture or context-aware common operational picture (Hwang and Yoon, 2020; Luokkala et al., 2016). The shared mental model and the common operational framework are absolutely essential to any effective response to a disruption by an organization (or group of organizations). Thus, when organizations carry out pre-established exercises simulating disruption scenarios or develop response scenarios for specific situations (called incident response playbooks), these two components of their SSA are precisely what they are attempting to develop.

Nevertheless, simulation exercises almost never require the organization to fully mobilize because of the obvious issues related to the fact that the organization must continue its daily operations during the exercises. For their part, incident response playbooks are often developed by a given OU to manage its own responses to incidents, but are often too general to be really effective (Stevens et al., 2022). Hence, although they are very important, exercises and playbooks are not sufficient to ensure that an organization responds effectively to a disruption that requires several OUs to intervene simultaneously (Tena-Chollet et al., 2017; Stevens et al., 2022).

Thus, even when a crisis cell is set up, if the organization has not previously acted to integrate the work done by the various OUs responsible for managing ARM, it will undoubtedly impair the OUs' ability to build a shared mental model of the situation to be solved (Tena-Chollet, 2012; Hwang and Yoon, 2020) and establish a common operational framework for the intervention (Hwang and Yoon, 2020; Endsley, 2015). This can give rise to a certain incoherence in the overall organization's response to incidents. Stakeholders then realize that roles and responsibilities are ambiguous or not widely known (Pilemalm and Yousefi, 2020); priorities are unclear or not shared (Micouleau et al., 2020); interdependencies among different functions (OUs or MCMs) have not been considered (Jean-Jules and Vicente, 2020; Amansou and Chaouki, 2019); information needed for decision-making is missing, inaccurate or out of date (Bharosa et al., 2010); or decisions that could be made quickly at an operational level must be made and endorsed at the top of the hierarchy, slowing down the response process (Schraagen et al., 2010) and introducing bias at every step of the decision-making process, especially when decisions must be made quickly and under stress (Sarker et al., 2016; Tena-Chollet et al., 2017). This bias can give rise to a dichotomy (or even conflict) between the different operational objectives to be achieved or between operational and strategic objectives (Micouleau et al., 2020).

This reality is aggravated by the fact that organizations now face more emerging risks. Characterized by high levels of ambiguity, uncertainty and complexity, emerging risks exploit any alignment of systems' vulnerabilities to propagate from one system to another and generate cascading failures that affect the entire organization and possibly others (Salim et al., 2021; Hopkin, 2018; Morabito and Robert, 2023b). It is very difficult to identify aligned vulnerabilities (or pathways offering less resistance to the propagation of failures) a priori since the complexity of the systems and their interdependencies means that the relation between a threat and an impact is not necessarily linear or directly causal (Morabito and Robert, 2023b; United Nations Office for

Disaster Risk Reduction [UNDRR], 2019). An impact is therefore the result not of a single event but of a combination of several contributing factors. To address these risks, an organization must obtain a more holistic view of risks and how they are mitigated (through the deployment of MCMs) and managed (by all OUs). To obtain such an overall perspective, the organization must be able to integrate all the information, but also uncertainties/unknowns, about threats, MCMs, assets and the impacts of their failure, and the roles and responsibilities of the OUs responsible for managing ARM within a single repository, such as the one illustrated in figure 7.6.

To do this, it is imperative to create preferential (Chionis et al., 2022) or cooperative spaces (Morabito and Robert, 2023a; Morabito and Robert, 2023b; Robert et al., 2007) – that is, cooperative structures – to allow the various OUs responsible for managing ARM to engage in discussions. When players are in contact with each other, it is possible to obtain a general picture of the organization's vulnerabilities that could not be obtained in any other way and to proactively identify the paths that offer the least resistance to failure propagation (Morabito and Robert, 2025). That is why, in most cases, post-accident analyses succeed in tracing the path taken by cascading failures and determining the series of events that led to the accident (UNDRR, 2019). And in many of these cases, analysts conclude that indicators (red flags) alerting players of a potential risk were present but, since they were not available within a common repository, they could not be correlated, aggregated, interpreted and reported correctly – what is also called risk data aggregation and risk reporting (Basel Committee on Banking Supervision, 2012). To use an analogy, all the pieces of the puzzle existed but, since they had not been assembled, it was impossible to see the overall picture, at least not until someone was given the mandate of putting the pieces together.

All these findings highlight the issue that function-based structure represents for large organizations that want to manage risks effectively; they also show the importance of IRM. Therefore, to effectively implement IRM, not only must an organization put in place a specific governance framework (Morabito and Robert, 2025) but it must also adopt a cooperative structure that can break down the organizational silos separating the OUs responsible for managing ARM.

7.5 The cooperative structure: enabling strategic and crosscutting integration of risk-related activities

Integration of risk management must achieve two main objectives. First, it must make it possible to align the organization's operational, tactical and strategic levels; that is, it must allow players to create the necessary alignment between the organization's strategic goals related to its mission and vision to the operational activities conducted to mitigate risks that might compromise those goals. To do this, the organization must put in place a common frame of reference composed of program charters, policies, directives, processes, norms and standards, and performance indicators (Morabito and Robert, 2025). This common frame of reference must allow to clarify the mission, objectives, and roles and responsibilities of all the OUs responsible for managing ARM in respect of the MCMs the organization has deployed to ensure that no activity required for the proper functioning of these measures is omitted (installation, financing, maintenance, inspection, training, monitoring, etc.). Morabito and Robert (2025) call this strategic (or vertical) integration of risk management.

Second, integration must allow the actions performed by all the OUs responsible for managing ARM to be coordinated and their information to be aggregated so to give the organization a more holistic view of the risks it faces and how they are managed. To do this, the organization must adopt an aggregation model (like the one shown in figure 7.6) that enables the players to develop their SSA of the risks the organization faces. This SSA is developed on the basis of the information contained in the aggregation model about threats, assets, the impacts of assets' failure, the MCMs deployed to mitigate risks, and each OU's roles and responsibilities in relation to the proper functioning of these MCMs. Morabito and Robert (2025) call this crosscutting (or horizontal) integration of risk management.

To achieve this twofold integration of risk management, this article proposes to combine within the same cooperative structure the 3LoD model and the concept of UE.

7.5.1 The 3LoD model and the concept of UE

Strategic and crosscutting integration of risk management can only occur if the organization has set up a cooperative structure that allows it to meet its integration objectives. The cooperative

structure for IRM proposed in this article is inspired by the IAA's 3LoD model and includes the concept of UE.

The purpose of the 3LoD model is to create and protect value for an organization and its stakeholders by implementing sound governance and risk management dispositions (Institute of Internal Auditors [IIA], 2020). To this end, the model provides for a three-line (or three-level) structure. The first line comprises operations related to the functioning of the MCMs that have been set up to mitigate risks (Autorité des Marchés Financiers [AMF], 2021). The second line includes the risk management and monitoring functions and compliance auditing. Its role is to provide advice regarding how well the MCMs set up to mitigate risks are aligned with the achievement of the organization's risk management goals (AMF, 2021). Finally, the third line covers the audit and internal auditing functions. It has the goal of providing objective and independent assurance of the overall effectiveness of risk governance and management (AMF, 2021). The 3LoD model will therefore be transposed to the IRM cooperative structure to create the necessary alignment between the organization's operational, tactical and strategic levels and thereby achieve the objective of strategic risk management integration.

The concept of UE refers to the implementation of a cooperative structure involving several independent stakeholders engaged in a common operation and striving to achieve a common objective (Greco, 1995; Kingsley, 2017a; Wilder, 2012). This concept is applied in the field of military and emergency management and becomes especially relevant when political, military, organizational and citizen-led initiatives are combined (Wilder, 2012). UE must be directed by a competent authority and is based on four key principles:

(1) a common understanding of the situation;

(2) a common vision of the objectives to achieve;

(3) a coordination of all the efforts to achieve these objectives; and

(4) a common measure of progress toward achieving these objectives (Kingsley, 2017a).

In these four principles, we recognize the concept of SSA, which entails a shared mental model (principles 1 and 2) and a common operational framework (principles 3 and 4). The concept of UE will therefore be transposed to the IRM cooperative structure to create alignment among the OUs

responsible for managing ARM and thereby achieve the objective of crosscutting risk management integration.

7.5.2 The cooperative structure

The transposition of the 3LoD model and the concept of UE to the cooperative IRM structure is reflected in the division of the organization's risk management activities among three levels and the implementation, at the tactical level (i.e., LoD2), of an IRM Team (IRMT). Figure 7.7 illustrates this cooperative structure. The following subsections explain how this structure works.

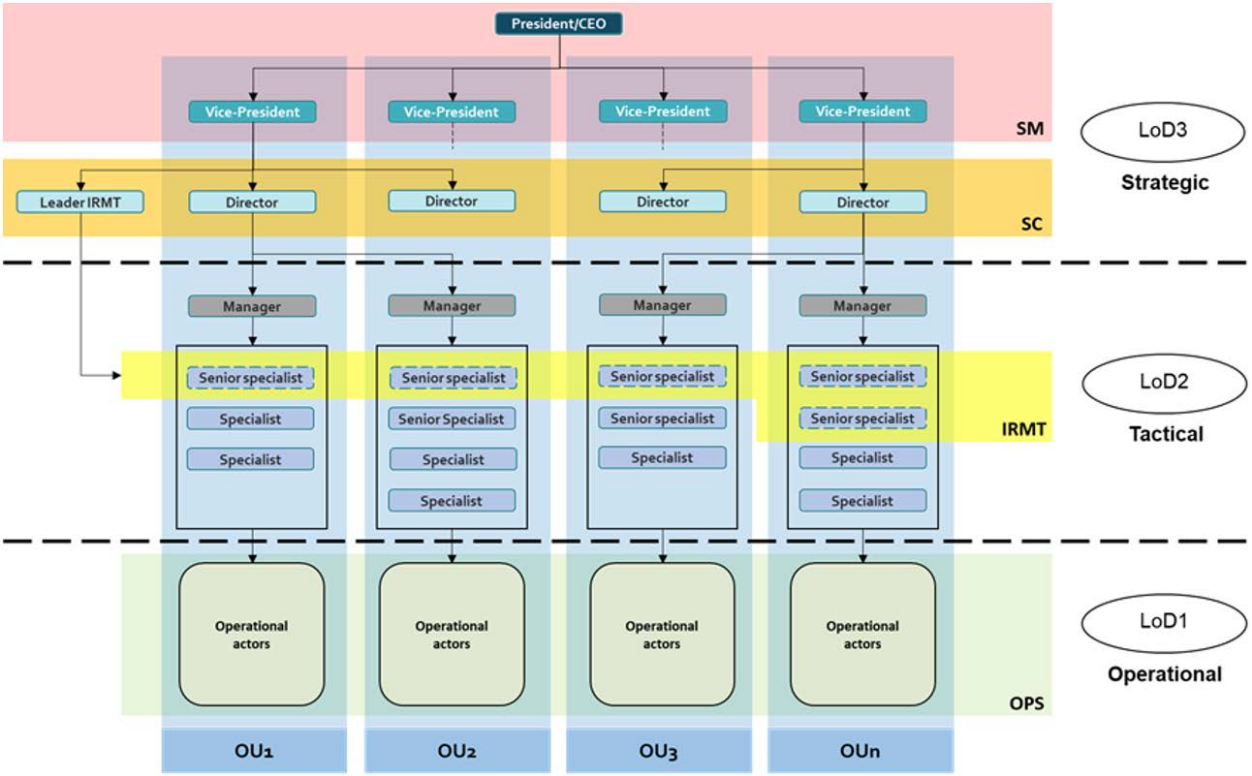


Figure 7.7 Cooperative structure for IRM

7.5.2.1 Operational level (LoD1) – OUs responsible for ORM

The first line of the cooperative structure corresponds to the operational level and concerns all the activities carried out by the OUs that are responsible for managing ARM and the MCMs' functioning. These activities comprise all the tasks related to monitoring the environment (threats) and all actions taken in respect of MCMs to ensure that they operate appropriately and thus fully meet the objectives for which they were deployed (as shown in figure 7.6). These activities are typically executed by the operators of the measures, who are responsible for ensuring that all

MCMs operate effectively and that all risk-related operational indicators, information, but also uncertainties/unknowns are relayed to LoD2. Subsequently, all the actions identified at LoD2 and LoD3 are decentralized to these operational players (LoD1).

7.5.2.2 Tactical level (LoD2) – IRMT

The second line of the cooperative structure corresponds to the tactical level and concerns all the activities related to MCM management and typically executed by the specialists in each OU responsible for managing an ARM. These specialists make sure that the measures comply with the organization's directives. This level is also where the IRMT is situated and where IRM occurs. At the tactical level, there is normally a good understanding of the organization's fundamental objectives (objectives that senior management wants to accomplish), and also of the operational objectives to be achieved, the functioning of operations and their related issues, which creates the necessary alignment between the organization's strategic, tactical and operational levels (Greco, 1995).

Guided by the concept of UE, the IRMT's role is to consolidate IRM governance by making sure that all the OUs responsible for managing ARM adhere to a common frame of reference. That is, they have defined their mission and objectives; that policies, directives, processes and standards are in place to support these missions and objectives; that performance indicators are identified to measure the effectiveness of all these measures; and, above all, that all these elements are coherently aligned and complementary and to ensure everyone is on the same page regarding what needs to be done and how to coordinate their efforts in order to achieve their goals (Edgar et al. 2021).

To do this consolidation work, the IRMT must necessarily be made up of experts from each OU responsible for managing an ARM. Thus, each OU is represented within the IRMT by an expert (two in some cases) who will create a link between their own OU and the IRMT. These players will then engage in a process of social construction of collective knowledge of risks to increase their SSA (Morabito and Robert, 2023b). This collective knowledge will give them a better understanding of the risks the organization faces and their management and enable them to suggest risk mitigation plans for the whole organization. It will also allow them to identify areas of uncertainty/unknowns in their understanding (areas of ignorance) that should be further investigated. Identifying these areas of ignorance is very important, especially in a context of

emerging risks, since such risks not only tend to develop in regions where the body of knowledge is poor/weak (Hopkin, 2018) but also have the capacity to cross knowledge borders (new or discipline-based knowledge) (Salim et al., 2021). This means that not only is multidisciplinary knowledge needed to identify them; in addition, transdisciplinary knowledge is required to understand them. This transdisciplinarity is necessary to understand complex problems and can only be developed if the people who have elements of the responses needed to solve these complex problems are brought together (Gooding et al., 2022), which emphasizes the importance of having a multidisciplinary IRMT.

The IRMT is mandated to focus almost exclusively on IRM. In concrete terms, the IRMT receives its inputs from the operational level, that is, the OUs responsible for managing ARM, in the form of operational information and indicators. The IRMT then does a number of analyses to integrate, aggregate and correlate these inputs and embody them in more aggregated, strategic risk indicators (e.g., key risk indicators), which give it a more holistic view of the risks the organization faces. When information is lacking, the IRMT carries out the necessary analyses to seek out missing knowledge or, if such knowledge is unavailable or inaccessible, flags these uncertainties as unknown parameters that need to be managed. The IRMT then passes these key risk indicators on to senior management, along with expertise and recommendations that will enable it to support strategic decision-making on how to manage these risks or adapt to real/anticipated changes in the environment. When senior management identifies or formulates problems or questions, the IRMT does the necessary analyses to find answers to these questions; when strategic decisions are being made, the IRMT embodies them into operational objectives that will be decentralized to the operational players (at LoD1) so they can take action.

The IRMT's experts play a crucial linking role between the organization's senior management (LoD3) and their colleagues in their own OUs (LoD1), which is why the IRMT is positioned at the tactical level (LoD2). Thus, on one hand, these experts are responsible for representing their own OUs' needs within the IRMT; on the other, they are responsible for ensuring that the results of the IRMT's work are conveyed to their respective OUs. This transfer of information allows risk management to be decentralized, as intended by IRM. For this reason, it is fundamental for the members of the IRMT to maintain their ties with their respective OUs. In that way, they will not be perceived as intruders "poking their noses" into the OUs' internal affairs when they interact with them, and they will always have access to up-to-date information.

The quality and success of the IRMT's work depend crucially on its members' competence. They need to have great expertise in their areas of practice and excellent knowledge of how their OUs work. They will typically be senior specialists in their respective fields (e.g., business continuity, emergency management, physical security, computer security, occupational health and safety, etc.). Also, they must be profoundly committed to the common cause (that is, IRM) and have demonstrated their autonomy. Above all, the members of the IRMT must possess a certain independence and neutrality so that their professional judgment is not influenced by operational, budgetary or other considerations or constraints. This is absolutely necessary for formulating relevant, impartial recommendations for the organization.

Depending on the risk being analyzed, the IRMT can ask for help from outside resources – that is, other colleagues – or in some cases from external consultants, for example to analyze specific problems that require knowledge that the IRMT's members do not have. Consequently, it can capitalize on all the individual knowledge available within the organization to ensure that the right people intervene at the right time. In this way, the IRMT's functioning corresponds to agile, organic functioning. This type of functioning is highly appropriate for initiatives that involve collaborative work, crosscutting integration and openness to partnership (Jacob and Michel, 2020). One of the advantages of agile, organic structuring is the freedom of action and reflection that this kind of structure allows (Jacob and Michel, 2020), which is required in an initiative like IRM.

7.5.2.3 Strategic level (LoD3) – Leader, steering committee and senior management

The third line of the cooperative structure corresponds to the strategic level. It concerns all the activities related to compliance audits and decision-making regarding the strategy to be applied to mitigate risks, adapt to real/anticipated changes in the environment, or intervene if necessary. This level is where the leader of the IRMT, the steering committee and senior management are located.

<u>Leader of the IRMT</u>

The leader is mandated to head up the IRMT. Together with the steering committee, the leader ensures that the IRMT's work is always aligned with the organization's strategic objectives. And together with the IRMT's members, the leader ensures that IRM fully incorporates and is appropriate for the operational issues. Consequently, the leader is responsible for setting the IRMT's major orientations based on the organization's priorities and operational needs. The leader is also responsible for reporting periodically to the steering committee and senior management to

present the advancement of the IRMT's work and an overview of the organization's posture in respect of the risks. During these reviews, the leader will share the recommendations the IRMT has identified to consolidate IRM-related governance (e.g., by reviewing or clarifying the goals and roles and responsibilities of the OUs responsible for managing ARM), reduce any risks deemed to be too high (e.g., by adding MCMs to certain assets), or adapting to real/anticipated changes in the environment (e.g., by anticipating certain investments related to adaptation to climate, social or technological changes or reviewing certain standards as a function of changes in legislation).

Without being an expert in all the IRMT members' practice areas (which would be difficult in any case), the leader must still have good multidisciplinary knowledge so he can inculcate a joint vision in the IRMT members and guide them in achieving that vision. The leader could be compared to an orchestra conductor, who need not know how to play all the instruments but must have a certain talent to unify the work of all the musicians in a harmonious whole. The analogy is that each OU must remain relatively independent in its internal functioning (like each musician in an orchestra), but that all the information and indicators that come from their work (i.e., emerge from ARM) should be coherently and harmoniously integrated/aggregated. Needless to say, the leader must be chosen carefully. According to Kingsley (2017b), a UE leader "must be a trail-blazer and skillful manager, [capable] of creating a clear path through a sea of ambiguity, confusion and discord." Thus, again according to Kingsley (2017b), this person must be visionary, respectful, inclusive and trustworthy. The leader must also have the necessary interpersonal skills to develop solid relationships and fully assume his role as a catalyst and unifier on the IRMT. It is also important for the leader to be demonstrably transparent and neutral (Morabito and Robert, 2023a). These two qualities are absolutely essential to create a climate of trust and a win-win context for all stakeholders involved in IRM.

In addition to these qualities, the leader must have acknowledged risk management skills to ensure that the work done is relevant, rigorous and credible. Finally, he must have some status (authority) within the organizational hierarchy: typically, the leader will have a role equivalent to the directors or vice-presidents (depending on the number of levels in the organization). In organizations that have a chief risk officer position or the equivalent, the leader would typically hold that position.

Steering committee

The steering committee is made up of the directors or vice-presidents (depending on the number of levels in the organization) of each OU responsible for managing an ARM. These have, of course, responsibilities that are directly related to the OUs' operations associated with MCMs proper functioning; when it comes to IRM, however, their role is to validate the IRMT's work by making sure that the team's objectives always allow the OUs to align their strategic, tactical and operational objectives.

The steering committee is responsible for identifying the experts who will serve on the IRMT and for acting as a facilitator to simplify established mechanisms that may be ill adapted to crosscutting initiatives. Thus, the steering committee can facilitate the transfer of information from one OU to another or authorize the use of additional resources when necessary (e.g., temporarily free up some resources from their regular functions to support the IRMT or reach out to external consultants). It is also up to the steering committee, with the agreement of senior management where necessary, to approve the implementation of the IRMT's recommendations. Finally, the steering committee may act as mediator to resolve conflicts, for instance in case of disagreement between the IRMT members and the leader.

Senior management

In the area of IRM, senior management is obviously responsible for making all the strategic decisions needed to guide the organization through changes in its environment and manage any risks affecting it so that it can always fulfill its mission and achieve its strategic objectives. To do so, it analyzes key risk indicators and the recommendations conveyed to it by the leader of the IRMT and the steering committee and uses these inputs to help with decision-making. However, senior management's greatest responsibility is undoubtedly to ensure that the IRMT's existence and legitimacy are entrenched throughout the organization, in a clear mandate that specifies the strategic importance the organization attributes to IRM and confirms the lasting nature of the cooperative structure. Without a commitment from senior management and a clear mandate, any IRM initiative within an organization is, sooner or later, doomed to failure (Morabito and Robert, 2023a).

7.6 Discussion and conclusion

In large organizations, ARM are most often executed by different OUs operating in silos. This means that risk-related information is dispersed throughout the organization and there is no real aggregation of this information within a common repository. In addition, decision-making regarding the actions required to mitigate risks are also dispersed throughout the organization and there is no one entity responsible for ensuring that all these actions are coordinated and coherent. Under such conditions, large organizations are often unable to optimally support their strategic decision-making processes related to risks because they do not have a holistic view of the risks they face and how they are mitigated/managed overall.

To remedy the situation, this article presents a cooperative structure for IRM that is well adapted to large organizations and makes it possible to achieve the crosscutting and strategic integration goals inherent in IRM. Established on the basis of work done within a large Canadian organization and inspired by the 3LoD model and the concept of UE, this structure centralizes IRM-related activities within a multidisciplinary, crosscutting IRMT, headed up by a competent leader. The primary goal of this structure is to allow these players to develop their SSA and to create value for the organization in providing it with recommendations and key risk indicators that will guide it in its strategic decision-making and that it could not obtain in any other way. To be truly effective, this cooperative structure must be set up within a broader IRM governance framework and the work of the IRMT must be strongly supported by the organization's senior management (embodied in a clear mandate) so that it has the legitimacy it needs to act and is able to fully express its professional judgment and make impartial recommendations to mitigate risks. However, in addition to a governance framework and a cooperative structure, IRM requires an integration model that will allow risk-related information to be aggregated, along with any uncertainties/unknowns that might exist regarding new risks – that is, emerging risks – into a coherent whole that is capable of generating new collective knowledge on risks and its related risk indicators. To that regard, the challenge is to ensure that the aggregation model illustrated in figure 7.6 can be used to generate this kind of indicator and ensure that these indicators are as objective as possible, reducing players' individual perceptions of risks. The issue of risk perception is particularly important in a context in which large organizations are composed of numerous players, all of whom may have different risk perceptions and tolerances that could affect, ultimately, organizational decision-making.

CHAPITRE 8 ARTICLE 5 : A KNOWLEDGE-BASED RISK-DATA AGGREGATION MODEL LEVERAGING SOCIAL CONSTRUCTIVISM AND SHARED SITUATIONAL AWARENESS TO IMPROVE DECISION-MAKING IN LARGE ORGANIZATIONS

Morabito, L. et Robert, B. (). 'A knowledge-based risk-data aggregation model leveraging social constructivism and shared situational awareness to improve decision-making in large organizations', *Int. J. Risk Assessment and Management*, Soumis pour publication le 6 juin 2025.

8.1 Mise en contexte et présentation de l'article

Au chapitre 3, il a été mentionné que l'une des principales difficultés liées à la gestion des risques émergents tient du fait que ceux-ci sont hautement incertains, ambigus et complexes. Cela, en raison de la forte part de méconnaissance qui entoure ces risques. Dans ces conditions, la perception qu'ont les acteurs de ces risques devient un facteur important dans la gestion de ces risques.

La perception est définie comme l'activité cognitive (mécanismes/processus mentaux) par laquelle l'humain prend conscience de son environnement, c'est-à-dire l'activité par laquelle l'humain reçoit et interprète les informations qui lui parviennent via ses sens (Habib et al. 2018). La perception engendre des erreurs systématiques dans le raisonnement que l'on appelle « biais de perception » ou « biais cognitifs » (Tversky et Kahneman, 1974). Les biais cognitifs jouent un rôle important dans la perception des risques chez les individus. Plusieurs facteurs sont à l'origine de ces biais. Parmi ces facteurs, certains sont liés à la nature de certains risques, alors que d'autres sont liés à des caractéristiques propres aux individus ou à leur vécu (Kouabénan et al., 2007; Wachinger et al., 2013).

Parmi les facteurs liés à la nature de certains risques, on note entre autres l'incertitude et l'ambiguïté (Kouabénan et al., 2007). Ces caractéristiques sont par ailleurs présentes chez les risques émergents dont l'un des principaux défis liés à leur gestion tient justement à la forte influence de la composante « perception » dans les perspectives qu'en ont les individus (OECD, 2003; Beghetto, 2021; Morabito et Robert, 2023b).

Parmi les facteurs propres aux individus, on note principalement l'âge, le sexe, le statut (personnel, professionnel, social), la culture et les croyances (Hergon et al., 2004 ; Kmiec et Roland-Lévy, 2014 ; Kouabénan et al., 2006). Ainsi, un même risque sera perçu différemment par un homme versus une femme, ou par un jeune versus une personne plus âgée. Parmi les facteurs propres au vécu des individus, on note entre autres les connaissances, les compétences, les expériences vécues et la confiance envers soi-même et les autres. Ainsi, la perception des risques peut être influencée par le niveau de connaissances (Hergon et al., 2004). De manière générale, plus un individu a de connaissances relatives à un sujet particulier, plus il sera en mesure de développer une certaine rationalité par rapport aux risques qui lui sont liés, contrairement à une personne ayant peu de connaissances du sujet, qui aura tendance à s'en méfier davantage ou à adopter un comportement plus risqué du fait de son manque de connaissances (relatives à des normes/processus ou des façons de faire, par exemple) ou de son incapacité à saisir le danger réel. La perception des risques peut aussi être influencée par les expériences vécues (Wachinger et al., 2013). Ainsi, certaines personnes ayant peu d'expérience avec une situation, un procédé ou une machine, par exemple, auront, selon leur nature, tendance à s'en méfier davantage ou, au contraire, à adopter un comportement plus risqué. Certaines personnes ayant vécu des situations difficiles seront aussi, selon leur nature, plus enclines à accepter de plus grands risques ou, au contraire, à en accepter moins. La perception des risques chez les individus peut aussi être affectée par la confiance, qu'elle soit envers soi-même, envers les experts ou envers les autorités (Cisternas et al., 2023). Si un individu a confiance en ses moyens et ses ressources pour faire face à un risque ou s'il a confiance que les personnes qui sont responsables de gérer ce risque sont crédibles et qu'elles prendront les bonnes décisions, alors sa perception de ce risque en sera certainement positivement impactée. L'inverse est aussi vrai. Par contre, lorsqu'en excès, la confiance peut générer un biais d'optimisme, un biais de supériorité (d'invulnérabilité) ou un mélange des deux qui peut conduire à une analyse erronée de ses capacités réelles (ou celles des autres) à affronter une situation donnée (Hergon et al., 2004 ; Institut pour une Culture de Sécurité Industrielle [ICSI], 2021). Ainsi, certains individus avec beaucoup de connaissances ou d'expérience avec une situation peuvent avoir tendance à minimiser les risques puisqu'ils surestiment alors leurs capacités réelles à leur faire face ou deviennent trop familiers avec ceux-ci (ICSI, 2021). Ils développent une accoutumance qui fait en sorte que leur niveau de vigilance diminue puisqu'ils ne sont alors plus en mesure d'apprécier les risques objectivement (Hergon et al., 2004 ; Wachinger et al., 2013).

La perception des risques peut aussi être influencée par d'autres facteurs, comme la distance – qu'elle soit physique ou géographique (Wang et al., 2021a ; Wachinger et al., 2013), temporelle (Kouabénan et al., 2007) ou psychologique (Shah et al. 2023) – ou l'amplification sociale (Skøt et al. 2021). Ainsi, la perception d'un risque par un individu sera différente si ce risque est géographiquement distant que s'il est situé tout près. On a notamment remarqué l'effet de la distance physique sur la perception des risques dans les grands projets d'infrastructures (ex.: barrage, gazoduc/oléoduc, usine chimique, etc.) avec la montée du phénomène *Not In My Backyard* (connus sous l'acronyme NIMBY) depuis le début des années 1980 (Wang et al., 2021a ; Jodelet, 2001). Malgré les besoins sociétaux et les retombées économiques potentielles pour les régions concernées, les personnes situées près de ces installations ont une perception de ces risques très différente de celles qui en sont géographiquement éloignées (Wang et al., 2021a). L'effet de la distance temporelle dans la perception des risques peut quant-à-elle s'observer dans le domaine de l'environnement, par exemple en ce qui concerne les risques liés aux changements climatiques (Wang et al., 2021b) ou dans le domaine de la santé, par exemple en ce qui concerne les risques liés à la consommation de produits du tabac (ICSI, 2021). Dans ces cas, comme les effets sont incertains et répartis sur une longue période, les individus ne parviennent pas à apprécier le risque à sa juste valeur ou à saisir l'urgence d'agir, reportant constamment les actions nécessaires à leur prise en charge (ICSI, 2021). Finalement, on peut remarquer l'effet de la distance psychologique sur la perception des risques en fonction de qui, au bout du compte, en subira les conséquences. Ainsi, la perception d'un risque sera différente si les conséquences sont répercutées sur des personnes qui sont inconnues à l'individu plutôt que si ces conséquences concernent des personnes qui lui sont proches ou lui-même (ICSI, 2021). De son côté, l'amplification sociale peut affecter la perception des risques, notamment parce l'information véhiculée et sa fréquence peuvent induire un stress (anxiété, peur) supplémentaire chez les individus (Skøt et al. 2021). Ainsi, la perception d'un risque pourrait être négativement impactée si ce risque fait l'objet d'une couverture médiatique disproportionnée et répétée dans le temps (Ju et You, 2022) ou si elle est amplifiée par un effet de masse (effet de groupe) (ex.: groupes de pression, réseaux sociaux, etc.) (Szántó et Dudás, 2022). Les effets de la couverture médiatique et les effets de groupe sur la perception des risques ont largement été démontrés lors de la pandémie de COVID-19 (Ferreira et al., 2022 ; Ju et You, 2022 ; Martelletti et al., 2022).

La perception des risques peut finalement être influencée par ce que Daniel Bernoulli a défini comme l'utilité espérée (Bernoulli, 1738). En réponse au Paradoxe de Saint-Pétersbourg qui soulève la question à savoir pourquoi certaines personnes refusent de jouer à un jeu de hasard alors que l'espérance mathématique de gain leur est favorable (voire, infinie), Bernoulli formule l'hypothèse que le gain lui-même n'a d'importance qu'en regard de l'utilisation qui peut être faite de la valeur en jeu ou du gain lui-même (Martinez, 2010). Ainsi, un individu pourrait accepter un plus grand risque si le coût lié au risque a une utilité significative pour lui ou si le produit de ce risque (en termes d'avantage) a une utilité significative en rapport aux inconvénients potentiels. Cela est directement lié au rapport coût/bénéfice relié à un risque (Barnett and Breakwell, 2001 ; Sjöberg, 2000). Ainsi, selon sa perception, chaque individu a une aversion au risque qui est différente. Alors que certaines personnes vivent très bien avec un niveau de risque plus élevé, certaines autres ont un niveau d'aversion au risque qui est beaucoup plus faible et ne sont donc prêtes qu'à accepter très peu de risques.

Ainsi, la perception des risques varie d'un individu à l'autre selon une multitude de caractéristiques/facteurs. Cela fait en sorte que deux individus, confrontés au même risque, pourraient adopter des comportements complètement différents, selon les caractéristiques/facteurs propres à chacun d'eux. Mais, la perception des risques varie aussi en fonction du contexte. Cela fait en sorte que le même individu, confronté au même risque, pourrait adopter un comportement complètement différent selon ce contexte, tantôt en sous-évaluant le risque, tantôt en l'évaluant correctement, tantôt en le surévaluant, selon les différents biais cognitifs[36] entrant en jeu au moment de la prise de décision, c'est-à-dire au moment où le risque se matérialise. Dans ces conditions, les décisions des acteurs en regard de la gestion des risques ne reposent plus nécessairement sur le savoir ou sur une analyse objective de données précises et factuelles, mais davantage sur le facteur humain, soit l'expérience, la perception, l'intuition et l'émotion alimentées par le contexte. Ces décisions sont donc enclines à beaucoup plus de subjectivité et donc, de remise en question (Tena-Chollet et al., 2017). Ainsi, sauf dans les jeux de hasard, il n'existe pas une valeur absolue d'un risque, mais il existe plutôt un risque perçu qui est un construit de l'esprit

[36] Les biais cognitifs ne sont pas les seuls à jouer un rôle dans la prise de décisions. Les biais motivationnels peuvent eux-aussi avoir une incidence sur la prise de décisions. Les biais motivationnels découlent des motivations des individus et de leurs objectifs et ont une influence sur la réflexion et la prise de décisions (Gardair, 2007).

humain dépendant de plusieurs facteurs influençant la perception qu'en ont les individus (Niget et Petitclerc, 2012).

Dans le cas des grandes organisations, la complexité liée à la prise en compte de la composante « perception » dans la gestion des risques est décuplée du fait que plusieurs acteurs sont impliqués dans cette gestion. Cela est d'autant plus difficile dans un contexte où ces acteurs sont répartis dans différentes UF responsables des AGR qui ont des rôles différents dans la gestion des risques. Or, la littérature s'accorde sur le fait que l'une des manières de réduire les effets des perceptions individuelles des acteurs dans les processus de prises de décisions est de permettre à ces acteurs de développer leur ISP. Pour cela, les ICII sur les risques qui sont réparties dans l'organisation doivent être agrégées en un tout cohérent permettant aux acteurs responsables de la GIR dans l'organisation de développer leurs connaissances et leur compréhension commune de ces risques. Pour y arriver, un modèle d'agrégation est nécessaire. Ainsi, en lien avec le troisième (et dernier) objectif spécifique de ces travaux de recherche (et troisième composante d'un EC), l'objectif de ce chapitre est de définir ce modèle.

L'article qui suit présente donc le modèle d'agrégation des ICII sur les risques qui est proposé dans cette thèse. Essentiellement, le modèle d'agrégation demeure le même que celui illustré à la figure 6.2, mais plutôt que d'être utilisé dans le contexte de la dimension gouvernance de la GIR, il est utilisé dans le contexte de la dimension technique de la GIR. L'article montre donc comment ce modèle peut être utilisé afin de permettre aux acteurs responsables de gérer les risques dans l'organisation de développer leur ISP, c'est-à-dire de développer une RMC des risques auxquels est confrontée l'organisation et d'identifier un COC pour leur gestion. Finalement, l'article ouvre sur la perspective de pouvoir utiliser des algorithmes informatiques ou l'Intelligence Artificielle (IA) afin d'aider à l'identification et à la priorisation des alignements de vulnérabilités potentiels et des chemins offrant une moindre résistance à la propagation des défaillances.

8.2 Abstract

Organizations face major changes in their environment, which are generating new risks. These 'emerging' risks present specific characteristics that mean they are difficult to address with traditional risk management processes. To handle such risks, more multidisciplinary, transversal risk management approaches are required. This so-called 'integrated' risk management is based on

an increase in the collective knowledge of the players responsible for managing risks within organizations. Such approaches require an aggregation model within which this knowledge can be integrated.

This article proposes such a model. It was developed based on work carried out in a large Canadian organization and is intended to give large organizations an enhanced understanding of the risks they face, thereby enabling them to better support their tactical and strategic decision-making in respect of the actions to be taken to manage risks.

Keywords: common operational framework, collective knowledge, integrated risk management, shared situational awareness, risk aggregation model, risk perception, shared mental model, social constructivism.

8.3 Introduction

Emerging risks are characterised by a very high level of uncertainty, ambiguity and complexity (International Risk Governance Council [IRGC], 2018). As a result, there are numerous misconceptions about these risks (Hopkin, 2018). Because of these misconceptions, the literature agrees that emerging risks are difficult to address with traditional risk management processes (IRGC, 2018; Morabito and Robert, 2023b; United Nations Office for Disaster Risk Reduction [UNDRR], 2019).

The literature also agrees that the characteristics of emerging risks (uncertainty, ambiguity and complexity) mean that the management of such risks by the organizational players responsible for managing them is more likely to be affected by these people's individual perceptions (Beghetto, 2021; IRGC, 2018; Kouabénan et al., 2007; Organization for Economic Co-operation and Development [OECD], 2003). These perceptions may be influenced by several factors that may be specific to individuals (e.g., age, sex, beliefs and culture) (Hergon et al., 2004; Kmiec and Roland-Lévy, 2014; Kouabénan et al., 2006), to their background (e.g., education, experiences, knowledge and skills) (Hergon et al., 2004; Wachinger et al., 2013), or to the particular context characterising the time when the effects of these perceptions become visible (e.g., cognitive biases, mass effects and psychological, geographic or temporal distance) (Cisternas et al., 2024; Ferreira et al., 2022; Ju and You, 2022; Martelletti et al., 2022; Shah et al. 2023; Skøt et al. 2021; Szántó and Dudás,

2022; Wang et al., 2021a; Wang et al., 2021b). Under these conditions, decisions are no longer necessarily based on an objective analysis of precise, factual data but more on human factors and context. This means that two different individuals facing the same risk, might have two completely different behaviours based on their perception of this risk; this also means that the same person, facing the same risk might have two completely different behaviours based on the context characterising the time when the risk materialises depending on the various cognitive biases in play at that particular moment. These decisions are therefore likely to be quite subjective and open to interpretation, questioning and human error (Hergon et al., 2004; Tena-Chollet et al., 2017). For a large organization, risk perception is therefore a major challenge that must be addressed.

In addition to players' individual perceptions, large organizations must deal with an additional difficulty. Indeed, in large organizations, which are made up of several business units, and several hundred (or thousand) people, risk management is generally divided among several Organizational Units (OUs), each one of which is responsible for managing an Activity related to Risk Management (ARM), such as business continuity, physical security, information security, occupational health and safety, environment, or emergency measures. Each OU therefore has its own knowledge, which enables it to monitor the risks that concern it and make decisions regarding the ARM it is responsible for. Since these OUs generally operate relatively independently, all this risk-related knowledge is dispersed throughout the organization, without necessarily being aggregated in a common repository. Thus, the organization has a fragmented perspective on different aspects of risk but no holistic overview of risks and how they are ultimately managed by means of all the actions taken by the various OUs responsible for managing ARM (Morabito and Robert, 2025). However, large organizations need this kind of general overview so they can better support their tactical and strategic decision-making related to risk management.

To do this, large organizations must implement Integrated Risk Management (IRM) frameworks. These frameworks make it possible to integrate all ARM and, ideally, ensure that the knowledge of risks that is dispersed within the organization is pooled to support risk-related decision-making (Morabito and Robert, 2025). Such pooling requires the organization to adopt a transversal aggregation model within which knowledge can be coherently aggregated and correlated to generate high-value-added collective knowledge.

This article proposes such an aggregation model for IRM. Adapted to the context of large organizations, this model leverages social constructivism to assist the players responsible for IRM in large organizations in constructing transdisciplinary collective knowledge of the risks their organizations face. Its objective is to allow these players to develop their Shared Situational Awareness (SSA), or in other words, obtain a common understanding of these risks, so they can jointly identify the actions needed to reduce them.

8.4 What is SSA?

According to Chionis et al. (2022), reducing the effects of perception on risk management depends on increased knowledge, since such knowledge increases the rationality and objectivity of players' reflections by enabling them to develop their SSA.

SSA is based on the concept of situational awareness. Situational awareness refers to the faculty whereby individuals become aware of their environment via information that comes to them through their senses (perception); translate this information into something intelligible based on their knowledge, skills and past experiences (representation); and anticipate events that are likely to occur (projection). These three actions (perception, representation and projection) allow an individual to take action, that is to make a decision and act on the situation (Endsley, 1988; 1995). Situational awareness is essential to decision-making, especially in complex and/or uncertain fields such as risk management (Tena-Chollet et al., 2017), and most of all the management of emerging risks, given the particular challenges their management poses (Morabito and Robert, 2023b).

To develop situational awareness, an individual must develop a mental model (or mental image, mental representation) of the situation they face. This mental model then allows them to understand the situation they are in and identify an operational framework (or action plan) to deal with it. The mental model and the operational framework are the two components of situational awareness (Tena-Chollet et al., 2017). Now, unlike situational awareness, which applies to a single individual, SSA applies to a group of persons. In this case, instead of using the terms 'mental model' and 'operational framework', we would use the expressions 'Shared Mental Model (SMM)' and 'Common Operational Framework (COF)' (Hwang and Yoon, 2020; Luokkala et al., 2017; Tena-Chollet et al., 2017). Thus, a SMM enables players to develop a common understanding of the situation they are in, which in turn means they can formulate a COF, namely a concerted, co-

ordinated action plan, to deal with it. However, building a SMM requires a common repository in which players can pool their information and knowledge on risks. Morabito and Robert (2025) call this common repository the aggregation model.

8.5 The aggregation model

Transversal (or transdisciplinary) knowledge of risks can only be generated if a mechanism for co-constructing such knowledge is in place in the organization (social constructivism principle) (Morabito and Robert, 2025). To that end, the players responsible for IRM within the organization must be given a common repository, within which the knowledge of risks dispersed throughout the various OUs responsible for managing ARM can be integrated. This integration (knowledge aggregation and correlation) will fuel the players' joint reflections, which in turn will permit them to generate new collective knowledge of risks. For that purpose, Morabito and Robert (2025) propose an aggregation model for IRM grounded in the concept of risk based on the trinity of hazards, vulnerabilities and impacts. Figure 8.1 illustrates this model.

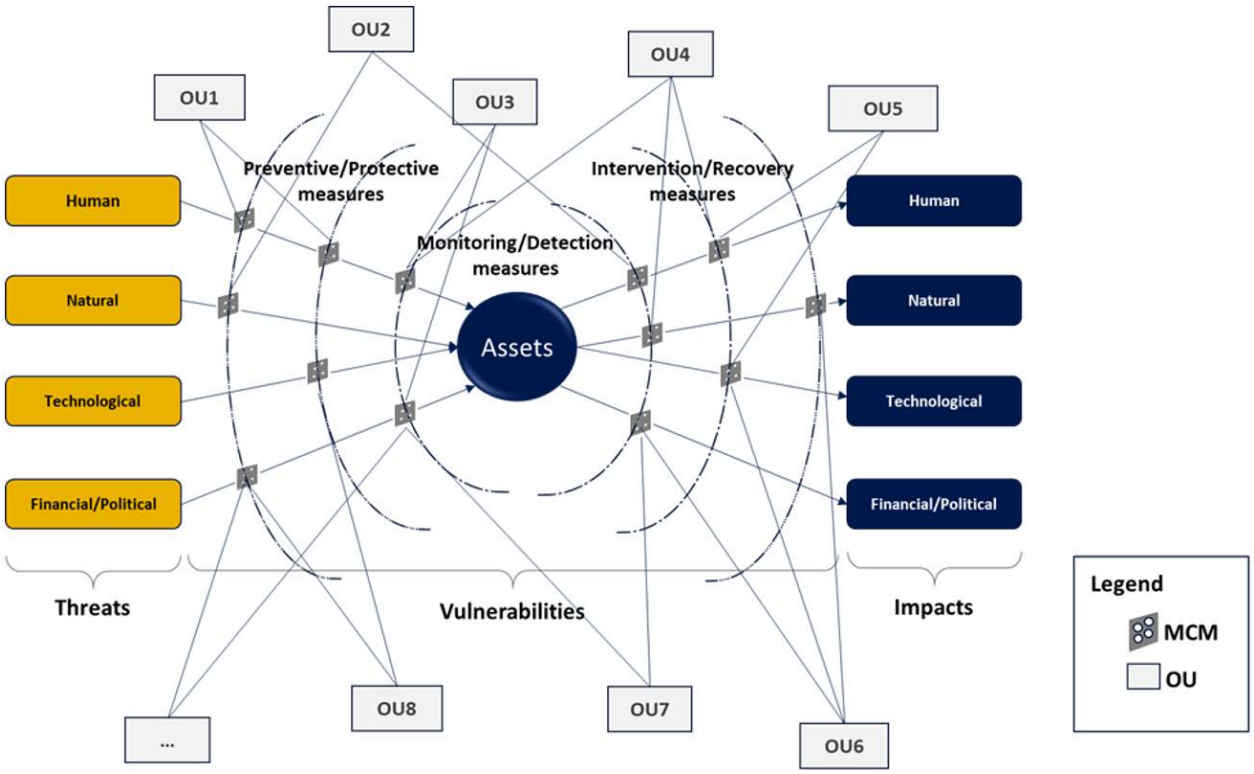


Figure 8.1 Aggregation model based on hazards, vulnerabilities and impacts

(Morabito and Robert, 2025)

In this model, an organization is considered as a system made up of several assets (positioned in the centre of the model). These assets represent all of the organization's tangible and intangible assets (e.g., information and knowledge, human resources, infrastructure and equipment, buildings, financial assets, etc.) (Business Lab, 2022) that it uses to execute the various functions that enable it to fulfil its mission, which may be reflected in the provision of a resource or a service (Robert et al., 2007).

Assets are subject to vulnerabilities. These may be inherent in the assets themselves (e.g., a piece of electrical equipment that is vulnerable to water) or may be the outcome of a deterioration of their condition due to external (e.g., climate) or internal (e.g., lack of maintenance) factors. Assets are also subject to the hazards of their environment. These hazards may also be external or internal to the organization and of varying natures (human, natural, technological and/or financial/political). They may affect assets directly or through domino effects. When that happens, it results in impacts that in turn can also be external or internal and of varying natures (human, natural, technological and/or financial/political) (Morabito and Robert, 2025).

To reduce risks, the organization deploys various Mitigation and Control Measures (MCMs). MCMs can be structural (e.g., generator, fence, etc.) or non-structural (e.g., training, procedure, etc.), and active (e.g., sprinkler, intrusion alarm, etc.) or passive (e.g., safety posters, emergency lighting, etc.). In addition, they may work for prevention and protection (to prevent hazards or protect assets), monitoring and detection (to monitor the environment and detect potential hazards or impacts), or intervention and recovery (to reduce the impacts of a disruptive event or restore normal functioning after a failure) (Morabito and Robert, 2025). In the aggregation model (figure 8.1), these MCMs are represented by the What-if model (Reason et al. 2006), and are therefore depicted as slices of Swiss cheese: the holes in the slices represent vulnerabilities (weaknesses or breaches) in these MCMs. A risky situation becomes possible when vulnerabilities align in such a way that a hazard can affect an asset and generate impacts.

To ensure optimal functioning of the MCMs, several OUs act on them. From the perspective of this sharing of roles and responsibilities, one OU may be responsible for identifying the MCM needed, another may be responsible for operating it, another for financing it, another for maintaining it, another for the associated training, etc. To ensure that the decisions and actions of the various OUs responsible for ARM are coherent, complementary and co-ordinated, it is therefore essential for the organization to ensure solid governance over the MCMs' functioning. For that purpose, Morabito and Robert (2025) propose an IRM governance framework for large organizations. This governance framework provides tools to clarify the OUs' roles and responsibilities related to the MCMs they deploy, measure the state of governance related to IRM, and identify the elements that must be improved to strengthen this governance.

However, to ensure that MCMs function optimally, not only must their governance be clearly established but the measures themselves must function correctly. Thus, where Morabito and Robert (2025) applied the aggregation model from the perspective of MCM-related governance, in this article the aggregation model will instead be used to characterise the general conditions in which MCMs exist. This information will then be applied to enable the organizational players responsible for IRM to develop their SSA regarding the risks the organization faces, that is, develop a SMM of the risks and put a COF in place to manage them.

8.6 SMM: From risk perception to risk representation

An organization can use the aggregation model presented in figure 8.1 to obtain an overall view of the risks it faces in respect of its different assets. To acquire this kind of perspective, the organization must develop its knowledge and understanding of the three risk parameters: the hazards that are present in the environment where assets are located, the vulnerabilities of these assets and the impacts of failure of these assets. However, the characteristics of emerging risks mean that it may be difficult to establish a causal relation between a hazard and an impact, since numerous intermediate phenomena may intervene between the two (Morabito and Robert, 2023b; UNDRR, 2019). In these conditions (where complexity, uncertainty and ambiguity prevail), the IRGC (2017) strongly recommends favouring risk management strategies focused on increasing resilience and reducing system vulnerability. A system's resilience and vulnerability are directly related to the MCMs that are deployed to protect it, enable it to function despite disruptions, and restore it quickly after a failure (Robert et al., 2019). Since these MCMs are only effective if they operate correctly, the players responsible for IRM must determine whether or not their conditions are satisfactory.

To do this, each MCM must be analysed according to several 'facets', which correspond to the various issues that must be considered to ensure that these measures function optimally. There are a minimum of six issues:

1) **governance** refers to the coherence of the roles and responsibilities of players involved with MCMs' function; Morabito and Robert (2025) proposed a method for assessing MCMs' governance;

2) **operational condition** refers to MCMs' structural condition, in the case of structural measures, or documentation condition, in the case of non-structural measures;

3) **training** refers to the training offered to organizational players who have a role to play in MCMs' functioning (implementation, operation, inspection, maintenance, etc.);

4) **inspection** refers to inspection of MCMs' structural condition, in the case of structural measures, or auditing of MCMs, in the case of non-structural measures;

5) **maintenance** refers to the maintenance of MCMs, in the case of structural measures, or updating of MCMs, in the case of non-structural measures;

6) **financing** refers to the financing required to ensure the optimal functioning of MCMs, including financing for MCM implementation, operation, training, inspection or maintenance, for example.

Thus, if the governance of MCMs is clearly established, they are in suitable operational condition, they are maintained and updated as they should be, the training given to people who interface with these MCMs is appropriate, they are inspected regularly to ensure that their operational condition is acceptable, and financing is adequate to ensure their optimal functioning, then, these MCMs should be in an overall condition that enables them to achieve the objectives for which they were set up and, ultimately, reduce risks for the organization.

Figure 8.2 illustrates an MCM's overall condition based on the status of the six issues. As in figure 8.1, the MCM is represented by a slice of Swiss cheese. Each issue is associated with a 'hole' in the slice of cheese. To determine the status of these issues, colour indicators are used (red = unsatisfactory; yellow = fair; green = satisfactory; grey = unknown).

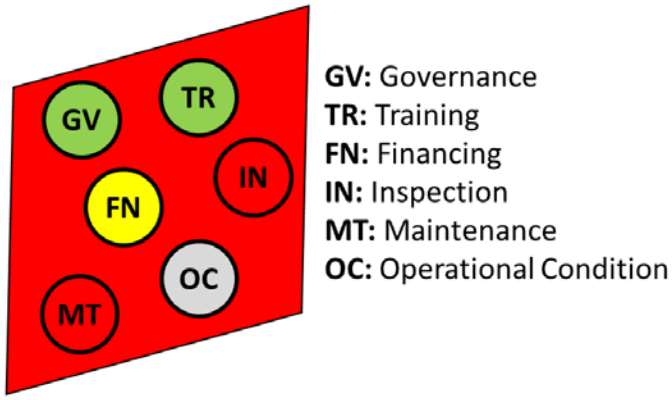


Figure 8.2 Representation of an MCM's overall condition based on the vulnerabilities affecting the six defined issues

In this example, we see that this MCM's overall condition is considered to be unsatisfactory (the slice of cheese is red). Thus, although the governance and training associated with this MCM are satisfactory, the financing of this measure is fair, inspection and maintenance are unsatisfactory, and its operational condition is unknown. One could therefore hypothesise that insufficient financing might explain why this MCM's inspection and maintenance are inadequate, which could in turn explain why its operational condition is unknown. Of course, this hypothesis would have to be validated, as there might be other explanations for this situation.

To obtain these ‘indicators’ associated with each MCM, the players responsible for IRM within the organization must consult all the OUs that have a role to play in MCMs’ functioning, namely the OUs responsible for ARM, but also the other OUs involved in the organization’s current operations. Internally, these OUs must conduct their own analyses, based on the parameters they consider important, to determine the status of the issues they are responsible for. Then, in light of all the information obtained from all the OUs concerned, the IRM experts must judge what condition the MCMs are in as a whole. This judgement must take into consideration not only the more objective parameters related to the status of MCM issues (and provided by the various OUs), but also more subjective considerations related to the individual perceptions of the players responsible for these measures. There are techniques to do this. For example, together with the OUs concerned, the IRM experts could weigh the various issues according to the importance the organization attributes to them. The Analytic Hierarchy Process (AHP) can be used to determine these weights. In such case, the relative importance of the issues (i.e., in relation to each other) could be disputed by the experts in the different OUs, specifically because of their individual perceptions of this importance. The Delphi method can then be used to obtain a consensus among experts taking into account the effect of their perceptions on the final results obtained for indicators. The combination of these two methods is called the AHP-Delphi technique and was employed during the work that lead to developing the risk-data aggregation model presented in this article. This technique is regularly employed to solve this kind of problem related to multicriteria ranking (Bagherigorji et al., 2022; Heydari et al., 2023; Nasiri et al. 2019; Taleai and Mansourian, 2008; Zhao et al., 2023). It should be noted that our objective in this article is not to present such a method but simply to illustrate the concept. Ultimately, it is the organization’s IRM experts who must determine the overall conditions of all MCMs based on the information the OUs provide about the status of the various issues and using the methods they deem to be most appropriate. In the end, the important thing is being able to distinguish the MCMs’ overall conditions and specifically which issues any vulnerabilities relate to. The results of these analyses can be compiled in an MCMs vulnerabilities matrix, an example of which is shown in table 1.

Tableau 8.1 MCMs vulnerabilities matrix (partial)

MCM	OUs responsible	Asset 1	Asset 2	Asset 3	Asset 4	Asset 5
MCM1		**1.67**	**2.17**	**2.00**		**?**
Governance	1, 3, 5	1	1	1	Not required	1
Training	1	1	2	1		2
Financing	3	3	3	3		3
Inspection	1	1	2	3		3
Maintenance	5	3	3	3		3
Operational condition	1	1	2	1		?
MCM2		**1.50**	**2.50**	**1.83**	**2.00**	**?**
Governance	2, 3, 4	1	1	1	1	1
Training	2, 3	1	3	3	3	2
Financing	3	2	3	3	3	1
Inspection	2, 4	3	3	1	3	3
Maintenance	4	1	2	1	1	3
Operational condition	2	1	3	2	1	?
MCMi		**1.83**	**2.00**	**1.67**	**1.67**	**?**
Governance	7, 8	1	1	1	1	1
Training	7	3	3	1	2	1
Financing	7, 8	2	3	3	1	3
Inspection	7	1	2	1	1	3
Maintenance	7	3	1	3	3	3
Operational condition	7	1	2	1	2	?
MCMx		**1.33**	**1.33**	**3.00**	**1.67**	**?**
Governance	3, 5, 6, 7	1	1	Non-existent but required.	1	1
Training	6, 7	3	1		2	1
Financing	3	1	3		2	3
Inspection	5	1	1		1	3
Maintenance	5	1	1		3	3
Operational condition	5	1	1		1	?

Legend: 1.0 to 1.5=green=low; 1.5 to 2.5=yellow=moderate; 2.5 to 3.0=red=high

In this example, the MCMs in effect for five different assets were assessed according to our six issues. To keep the example simple, we consider that all the issues have the same relative importance. The overall condition of each MCM is therefore determined as a function of the arithmetic mean of the results obtained for the issues. Thus, in this example, MCMx is in an overall condition deemed to be satisfactory in respect of Assets 1 and 2 (low vulnerability index of 1.33); in an overall condition deemed to be unsatisfactory in respect of Asset 3 (high vulnerability index of 3.00) (since the measure does not exist but is needed); in an overall condition deemed to be fair in respect of Asset 4 (moderate vulnerability index of 1.67); and in an unknown overall condition in respect of Asset 5 (unknown vulnerability index, '?') (since the measure's operational status is not known). Recall that a much more complex calculation mechanism using the AHP-Delphi technique (or any other technique chosen by the IRM experts) could be used but, as we mentioned, our objective in this article is not to propose such a calculation mechanism. Furthermore, it would be more beneficial for an organization that wishes to adopt such an approach to start with a very

simple calculation mechanism (e.g., the one presented here), which can be made more complex over time, as the organization's IRM experts get more familiar with the approach and as the organization's maturity towards IRM increases.

The MCM vulnerability matrix allows the players responsible for IRM to gain a high-level view of the overall condition for each MCM for each asset. Thus, when we analyse MCM1 in respect of Asset 1 and from the perspective of OU1, it is in a satisfactory condition since all four issues that concern it (governance, training, inspection and operational condition) are in a satisfactory condition (=green=1). On the other hand, the same MCM, seen from the perspective of financing by OU3 or of is maintenance by OU5 is in an unsatisfactory condition (=red=3). Thus, by combining the knowledge of OUs 1, 3 and 5, the players responsible for IRM will obtain a more comprehensive picture of this MCM's overall condition based on the status of all the issues. They will then be in a better position to determine vulnerabilities (weaknesses or breaches) in respect of this MCM that could represent a potential risk for the organization. Viewed as a whole, then, the matrix gives the players responsible for IRM and the OUs responsible for these MCMs a SMM of asset vulnerabilities based on the individual vulnerabilities of the MCMs deployed there. This result is only possible because of the aggregation of information and knowledge from all the OUs that have a role to play in the proper functioning of these measures, particularly the OUs responsible for ARM, but also other OUs within the organization, such as those responsible for operations.

Collective knowledge of the MCMs' conditions allows users to make more tactical and strategic observations. For example, regarding MCM1, we see that maintenance is systematically unsatisfactory for all assets. We also see that the financing associated with this MCM is unsatisfactory for all assets. Is there a systemic financing problem affecting this measure that means that it is not maintained the way it should be? Or is maintenance perhaps considered too complex and costly, so the organization has chosen to replace this MCM only when it actually fails? Or could the two factors not be related at all and there are other reasons for this situation? The response is important since, depending on the reasons underlying it, decisions regarding actions to correct the situation will not necessarily be the same: the organization might possibly invest more money in this measure to maintain it better, it could opt for a lower-maintenance replacement solution, or it could implement additional MCMs to make sure it can mitigate any potential impact of this measure's failure.

Another analysis, regarding Asset 5 this time, reveals that there is a zone of uncertainty regarding the condition of all the MCMs for this asset (represented by a '?' or grey area, in table 1). We can also see that maintenance and inspection of this asset are consistently unsatisfactory for all MCMs. These observations should raise questions in the minds of the experts responsible for IRM. Is this asset located in a distant area, so that access to it is difficult? If that is the case, it could also indicate that, if there were an emergency at this asset, an intervention would take a long time. By discussing the issue with the OUs concerned, the players responsible for IRM can better understand the situation and be in a position to make informed recommendations to the OUs concerned and senior management. For example, if the analysis with the OUs concerned confirms that the situation has indeed arisen because the asset is located in a distant or isolated region, then the players responsible for IRM could recommend that the preventive and protective MCMs in place be strengthened, that additional MCMs be implemented, or that intervention plans specific to this asset be developed, for example.

Beyond the analyses one can make directly from table 1, one can use the collective knowledge contained in this table to generate new, more transdisciplinary collective knowledge that will add more value to the analyses and add to the understanding of risks. To do this, the players responsible for IRM must incorporate the knowledge contained in table 1 into the aggregation model illustrated in figure 8.1 to build a SMM of asset vulnerabilities that is based on the overall condition of each existing MCM. Figure 8.3 shows the result of this action for Asset 1.

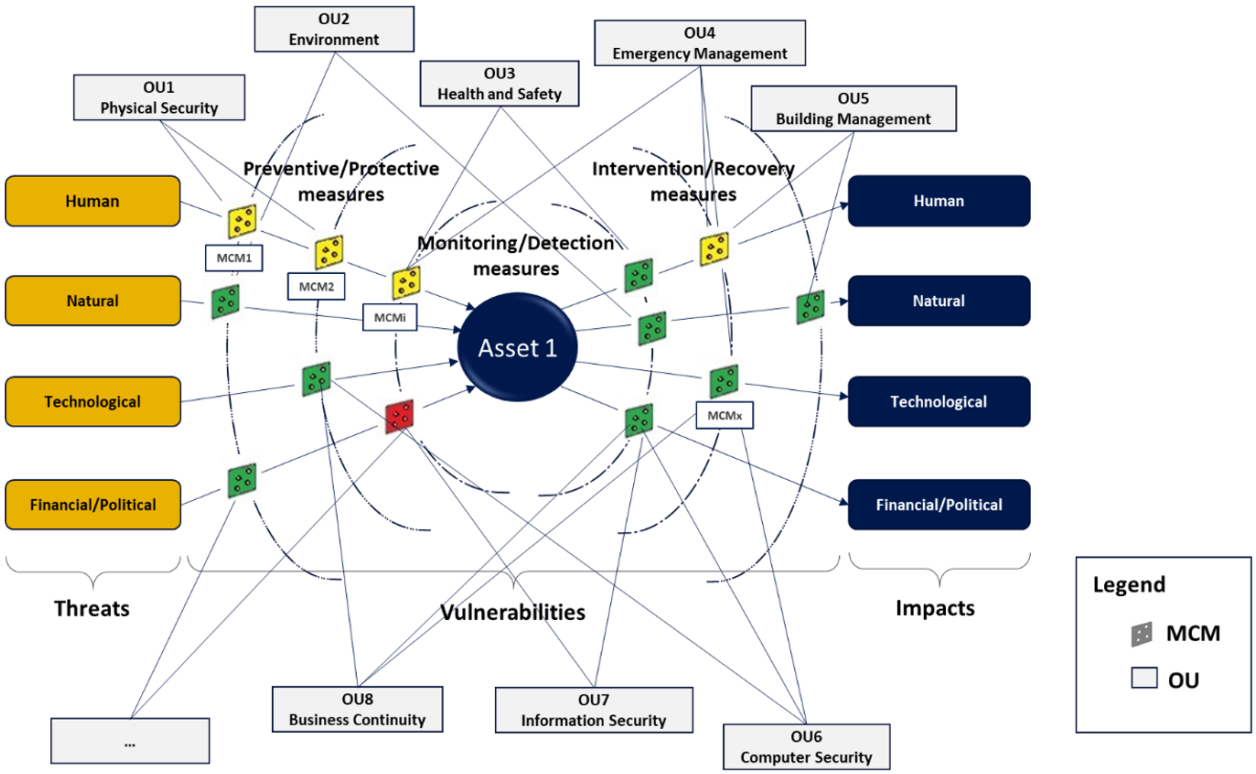


Figure 8.3 SMM of the vulnerabilities of Asset 1

In this figure, we suppose that all of Asset 1's MCMs were assessed and positioned in the model based on whether they concern prevention and protection, monitoring and detection, or intervention and recovery. It should be noted that a given MCM could be located in several places in the model because it could have several functions. Each MCM is also represented in the colour of the indicator that corresponds to its overall condition (from table 1). Thus, in figure 8.3, we see MCMs 1, 2 and i in yellow and MCMx in green. Proceeding in the same way for all assets, the experts responsible for IRM can obtain an overall picture of the vulnerabilities affecting the organization's various assets that they can then analyse to better understand the risks those vulnerabilities pose. Based on the results of their analyses, they can then suggest a COF to the OUs concerned and senior management to manage these vulnerabilities.

8.7 The COF: From risk representation to projection of anticipated situations

The SMM enables the players responsible for IRM in the organization to project potentially disruptive situations and identify the paths that offer lower resistance to the propagation of failures

(i.e., paths where vulnerabilities are aligned). For example, considering the SMM in figure 8.3, we see that no MCM exists to detect the occurrence of natural or technological hazards for this asset. For the people responsible for IRM, this suggests that the organization would be unable to detect a disruption related to one of these kinds of hazards until the impacts had happened. Thus, in such a situation, the organization could only respond reactively to the event. As for impacts, we see that the MCMs that detect impacts are all acceptable, but that the ones involved in intervention and recovery are mostly only fair. For the players in charge of IRM, that should raise questions about the organization's response capacity at this asset and would justify recommending that intervention and recovery mechanisms be strengthened. If that is not possible, for example because the asset is in a remote or isolated region, the players could recommend implementing much stronger prevention and protection measures and prioritising the recovery of MCMs involved in detecting and monitoring hazards, thereby adopting a more proactive attitude in managing incidents affecting this asset. If such solutions are not possible, the players responsible for IRM could request that a comprehensive analysis of the impacts of a failure of this asset be conducted. Depending on the results obtained, they could then recommend various solutions to reduce the impacts (e.g., redundancy or looping measures), transfer certain activities or critical equipment to other, less vulnerable sites, or, in an extreme case, relocate the asset to a more easily accessible area. Objective is then to come up with a COF that is agreed upon by all concerned OUs and senior management.

The SMM in figure 8.3 also allows to identify the paths where there are very few MCMs. For example, we see that the Natural hazards–Asset 1–Technological impacts and Natural hazards–Asset 1–Financial/political impacts paths have very few MCMs in place. The same is true of the Technological hazards–Asset 1–Technological impacts and Technological hazards–Asset 1–Financial/political impacts paths. In these conditions, it is very likely that the failure of one of the MCMs on these paths would result in impacts for the organization. Together with the OUs responsible for ARM, the people in charge of IRM could analyse the possibility of implementing other MCMs to make these paths less vulnerable to failures and increase this asset's resilience on these paths.

Finally, the SMM in figure 8.3 also allows to identify paths with several MCMs, which may seem relatively invulnerable a priori, but which actually present aligned vulnerabilities that could represent a potential source of risks. For example, if we examine the Human hazards–Asset 1–

Technological impacts path, for which the MCMs were assessed in table 1, we can conceptualise the potentially aligned vulnerabilities on this path, as shown in figure 8.4.

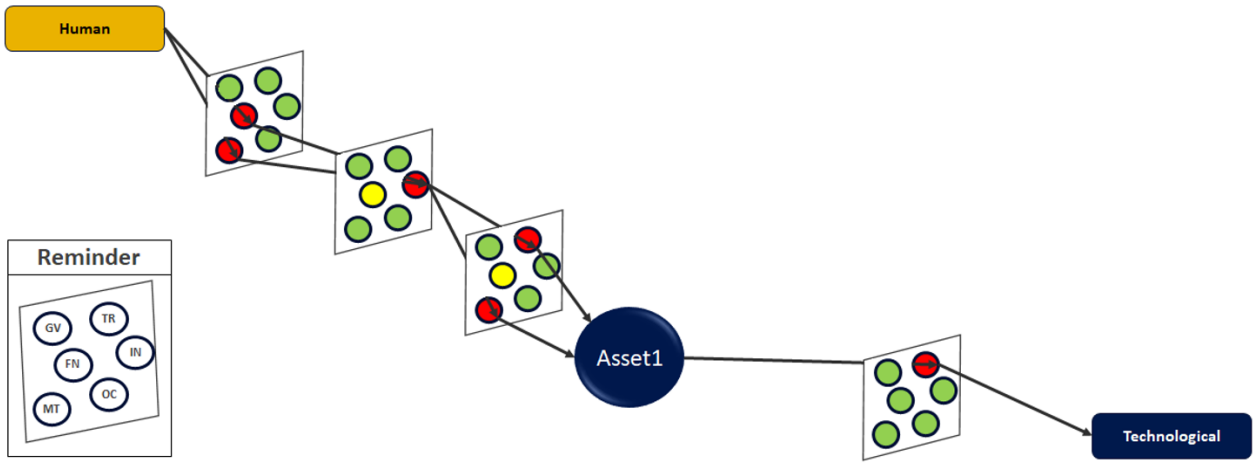


Figure 8.4 Conceptualisation of aligned vulnerabilities on the Human hazards – Asset 1 – Technological impacts path

For the players responsible for IRM, this representation reveals where (which MCMs and which issues) aligned vulnerabilities could let failures propagate. Thus, the analysis of the alignment of vulnerabilities indicates that a lack of financing, maintenance, inspection and training in respect of the MCMs contributing to the protection of Asset 1 from human hazards mean that this asset might be affected by a hazard of this type. If that were to happen, a lack of training related to the functioning of the MCM involved in intervention and recovery could mean that incorrect operation of this MCM would result in technological impacts. By repeating this exercise for all assets, the players responsible for IRM will be able to identify all the paths that offer low resistance to the propagation of failures (i.e., those with the most alignments of vulnerabilities). By working with the OUs concerned with these measures, these people will gain a better understanding of all the most vulnerable paths and can then conduct more specific analyses and seek out additional knowledge about the hazards that could exploit those vulnerabilities and the potential impacts if such hazards appeared. This additional knowledge can then be used to further expand their understanding of the dynamic whereby failures propagate along paths and generate new transdisciplinary collective knowledge, which will help the organization better understand the risks it faces. It could also help these players identify problems that are specific to certain MCMs or systemic throughout the organization (e.g., underfunding of certain maintenance programs or lack of training). This knowledge will then constitute an additional decision support tool regarding the

tactical and strategic actions to be taken to ‘close off the paths of least resistance’ that could become vectors for the propagation of a failure within the organization and possibly other organizations (through domino effects). They will then be able to recommend common and concerted action plans (i.e., COFs) to the OUs concerned and senior management to solve the problems based on their priority.

Eventually, a cyclic, incremental collective knowledge creation process will be developed within the organization, enabling new knowledge to be continuously generated until players have a transdisciplinary understanding of the problems related to aligned asset vulnerabilities and the resulting risks (Kuraoka et al., 2020). Thus, as knowledge and understanding increase, the uncertainties, ambiguities and complexities related to risks decrease in tandem. Of course, new risks will appear, but it will then be possible to address them in the same way, namely with the development of a true risk culture based on the co-construction of transdisciplinary collective knowledge of those risks (social constructivism principle) and on the increase in the collective understanding of these risks and how to handle them (SSA principle).

8.8 Discussion and conclusion

This article presented an aggregation model for risk-related knowledge for large organizations. Based on the principles of social constructivism and SSA, this aggregation model is intended to enable players responsible for IRM in large organizations to develop a SMM of the risks the organization faces that will in turn allow them to identify a COF to mitigate those risks. The objective of this model is to enable these players to increase the organizational collective knowledge of risks so they can better understand them and, consequently, better identify the actions needed to mitigate them.

However, the use of this aggregation model presents two issues. The first is related to the operationalisation of such a model. Recall that IRM requires co-operation by all the OUs responsible for ARM, but also by the OUs involved in current operations, throughout the organization. For that to work, an IRM governance framework must necessarily be in place in the organization (Morabito and Robert, 2025). In addition, a co-operative structure that favours transversal (i.e., among OUs) and vertical (i.e., among the organization’s operational, tactical and

strategic levels) exchanges must also be in place within the organization. For such a structure to be effective, it must rest on the existence of a competent and transversal team dedicated to IRM.

The second issue concerns the identification of paths offering the least resistance to failure propagation. Once the IRM experts and the OUs have compiled information about the various issues related to MCMs, an analysis must be done to identify the MCMs' vulnerabilities, their overall condition and the possible alignments of vulnerabilities, and thereby make it possible to identify potential risks and prioritise actions to reduce them. The example illustrated in this article is a very simple one. However, the task soon becomes complicated in a large organization with numerous assets, numerous OUs and numerous MCMs. Players then have to manage a vast amount of data. Moreover, depending on the problem to be analysed and the analysis context, the knowledge to be aggregated is not necessarily the same. And, like the organization itself, the environment and the context are dynamic, so this aggregation must be constantly updated to ensure that the results are in accordance with the reality at the time.

In this context, it could be useful to turn to artificial intelligence (AI) in order to benefit from AI systems' processing capacities. Computer algorithms designed to reproduce IRM experts' reasoning could greatly accelerate information processing. Such tools could, for example, be used to optimise the weighting of the different parameters linked to issues, speed up the identification of paths of least resistance to failure propagation, and help prioritise the different paths based on the risk they represent for the organization. AI tools could practically allow analyses to be conducted in real time, as and when basic knowledge is updated by the players responsible for IRM and those in the other OUs involved. Beyond the ability to obtain new knowledge in quasi-real time, such tools could also allow for reverse-engineering risk analyses: by varying the MCMs' conditions (and the status and weight of the various issues), AI tools could help represent possible future conditions that would generate failures and predict potential risk situations before they crop up, contributing to the creation of resilient-by-design systems. The value these tools could add to large organizations – and to society, which ultimately suffers the consequences of large organizations' failure – would therefore be enormous. Needless to say, further work is necessary before we get to that point, but it appears quite clear that coupling this aggregation model with AI capacities would present the potential for interesting research into more effective, proactive ways of managing risks, especially the most uncertain and complex ones, such as emerging risks.

CHAPITRE 9 DISCUSSION GÉNÉRALE

Ce chapitre se veut une discussion générale des travaux de recherche et vise à porter un regard critique sur les résultats obtenus, mais aussi, plus généralement, sur la manière dont la recherche a été conduite et qui aurait pu avoir une incidence sur ces résultats. Pour cela, la section 9.1 vise à faire une synthèse des travaux effectués et à revenir sur les objectifs de la recherche pour apprécier globalement dans quelle mesure ceux-ci ont été atteints. La section 9.2 vise à mettre de l'avant les apports scientifiques de cette recherche au niveau du domaine de la gestion des risques. Finalement, la section 9.3 présente les principales limitations de cette recherche et propose, par le fait même, quelques recommandations concernant des perspectives de projets qui permettraient d'adresser ces limitations.

9.1 Synthèse des travaux

La rétrospective du projet DOMINO présentée à l'article 1, *Success factors and lessons learned during the implementation of a cooperative space for critical infrastructures*, est le point de départ de ces travaux de recherche doctorale. Celle-ci suggérait que pour aborder la complexité des nouveaux risques, donc les risques émergents, des EC multiorganisationnels permettant aux grandes organisations de gérer les risques de manière plus intégrée doivent être mis en place. Or, cette rétrospective suggérait que l'un des freins associés au maintien sur le long terme d'un EC multiorganisationnel dédié aux risques était que les grandes organisations n'avaient pas encore elles-mêmes réellement adopté la GIR dans leur pratique. Ce constat était d'ailleurs renforcé par les observations faites chez l'organisation partenaire et par la publication de Jean-Jules et Vicente (2020) qui confirmait l'existence de cette problématique auprès de plusieurs grandes organisations. L'article 1 était donc important pour ces travaux puisqu'il a permis de prouver le potentiel des approches coopératives dans leur capacité à aborder les risques émergents, mais il a surtout permis d'identifier qu'un travail en amont au sein des grandes organisations était nécessaire afin de permettre à ces approches de s'inscrire dans la durée. Ainsi, cet article a permis de contextualiser ces travaux de recherche et d'identifier une avenue de recherche intéressante en la GIR chez les organisations de grande ampleur. Par le fait même, il a permis de poser l'hypothèse spécifique qui

allait guider le reste des travaux, à savoir que le concept d'EC, développé par le CRP pour permettre aux IC présentes à Montréal d'échanger des informations pertinentes sur leurs dépendances mutuelles afin de trouver une solution à la problématique des interdépendances entre les IC, pourrait être transposé à l'interne des grandes organisations pour aborder cette problématique de la GIR.

À ce stade, il devenait donc essentiel de présenter les concepts de risques émergents et de GIR et de les mettre en perspective des concepts traditionnels de risque et de gestion des risques. L'article 2, *Challenges related to emerging risk management*, visait cet objectif. Ainsi, cet article a pu expliquer les différences majeures qui existent entre le risque traditionnel et le risque émergent et a pu démontrer les limites de la gestion de risques traditionnelle lorsque confrontée à la complexité des risques émergents. Il a aussi pu établir que la forte incertitude de ces risques fait en sorte que ceux-ci doivent être adressés de manière globale et intégrée par l'organisation (donc en mettant de l'avant la GIR) et dans une optique d'accroissement de la connaissance et de la compréhension de ces risques de la part de tous les acteurs impliqués dans leur gestion. Ce faisant, l'article exposait les deux principaux concepts qui allaient être au coeur des travaux de recherche, et qui participent largement à l'originalité de ces travaux et à celle du cadre de gouvernance pour la GIR proposé dans cette thèse, à savoir le socioconstructivisme et l'intelligence situationnelle. Finalement, l'article a pu établir que la GIR est avant tout une question de gouvernance relative à la manière dont les grandes organisations gèrent les risques par le biais de leurs UF responsables des AGR. L'article présentait alors les éléments clés qu'un cadre de gouvernance pour la GIR devrait considérer (éléments qui sont présentés à la figure 3.3). Ainsi, l'article 2 a été fondamental pour cette thèse puisqu'il a permis de clairement établir la problématique de recherche, mais aussi, et surtout, d'identifier l'angle sous lequel cette problématique allait (voire, devait) être abordée dans le cadre de ces travaux de recherche.

Une fois la problématique de recherche établie et l'axe de recherche déterminé, il fallait identifier les objectifs que ce projet de recherche allait poursuivre. L'objectif général de ce projet découlait directement des articles 1 et 2 et consistait à développer un cadre de gouvernance pour la GIR chez les organisations de grande ampleur. Et, pour atteindre cet objectif général, l'article 1 suggérait d'adapter le concept d'EC développé dans le cadre du projet DOMINO. À ce stade, il fallait donc expliquer les principales caractéristiques d'un EC et voir comment celles-ci pouvaient être traduites

en objectifs spécifiques à atteindre. C'est ce que visait la section 4.2, à la fin de laquelle, les trois objectifs spécifiques de ce projet de recherche ont pu être établis, à savoir :

1. Établir le référentiel commun unissant les UF responsables des AGR. Ce référentiel commun devait fournir à ces acteurs une RMC de la problématique commune à résoudre (la GIR) et leur permettre de clarifier leurs rôles et leurs responsabilités en lien avec cette problématique et d'établir un CRC pour leurs actions.
2. Établir la structure de coopération permettant de supporter les échanges d'informations entre les UF responsables des AGR. Cette structure devait permettre de faciliter les échanges horizontaux et verticaux des informations sur les risques et s'arrimer de manière harmonieuse à la structure fonctionnelle des grandes organisations.
3. Établir le modèle d'agrégation des ICII sur les risques. Ce modèle devait permettre de construire une connaissance collective nouvelle et transdisciplinaire sur les risques capable de mieux supporter les processus de prise de décisions plus tactiques et stratégiques à l'égard de la gestion des risques.

Une fois les objectifs clairement établis, il fallait déterminer la méthodologie de recherche qui allait être utilisée pour mener ces travaux de recherche. C'est ce que visait la section 4.3. Clairement ici, comme une organisation partenaire allait être impliquée dans ces travaux et que l'intérêt était de développer un cadre de gouvernance qui soit viable autant en théorie qu'en pratique (donc, un cadre qui soit opérationnel), le choix de la méthodologie s'orientait de soi vers une approche de recherche axée sur les objectifs et de type appliqué. Aussi, comme une équipe d'experts de l'organisation partenaire allait travailler conjointement avec le chercheur, une méthodologie de recherche participative était davantage appropriée à ce contexte. Finalement, comme le chercheur allait être activement impliqué dans le volet pratique du projet de recherche et que les actions menées sur le terrain visaient non seulement une transformation des comportements des acteurs, mais aussi une transformation des façons de faire de l'organisation, la recherche-intervention devenait le choix tout indiqué pour cette recherche.

Avec l'axe de recherche déterminé et la méthodologie de recherche identifiée, la table était mise pour lancer les travaux de recherche. À ce stade, une revue de la littérature était nécessaire afin de valider la pertinence de la question de recherche (voire, la préciser ou la réorienter au besoin), mais aussi afin de permettre de mieux apprécier l'originalité de ces travaux de recherche et, à terme, de

la solution proposée en regard de l'existant. Ainsi, la revue de la littérature devait permettre de poser un regard assez large sur la GIR et sur les possibles manières disponibles aux grandes organisations de la mettre en place. Parmi les éléments d'intérêt qui ressortaient du lot en faisant une recherche sur la GIR, on retrouvait principalement des outils, des normes et des standards, des cadres de gestion des risques et des politiques, des guides et des lignes directrices. La revue de la littérature a donc porté sur ces différents éléments et a permis de confirmer le besoin pour un cadre de gouvernance spécifique à la GIR chez les organisations de grande ampleur qui soit plus pragmatique et qui aborde toutes les dimensions de la GIR, soit la dimension liée à la gouvernance, la dimension technique et la dimension humaine des risques. Elle a aussi confirmé que d'aborder cette problématique en utilisant le concept de risque basé sur l'incertitude et sous l'angle de la co-construction de la connaissance collective transdisciplinaire et de la compréhension de l'organisation des risques auxquels elle est exposée (donc en mettant de l'avant les concepts de socioconstructivisme et d'intelligence situationnelle) était une avenue tout à fait originale d'aborder cette problématique.

Maintenant que la revue de la littérature confirmait l'existence d'une problématique réelle et la possibilité de trouver une solution originale à cette problématique, il fallait répondre aux objectifs spécifiques de cette recherche. Ainsi, chacun des articles présentés aux chapitres 6, 7 et 8 a permis d'aborder un des piliers du cadre de gouvernance pour la GIR chez les organisations de grande ampleur proposé dans cette thèse.

Les travaux réalisés dans le cadre du chapitre 6 et l'article *A governance framework for achieving transversal and strategic integration of risk management in large organizations* ont permis d'établir le référentiel commun unissant les UF responsables des AGR. Ce référentiel commun est constitué d'une RMC du concept de risque et de la problématique de la GIR et d'un CRC pour les acteurs et leurs actions. Ainsi, ces travaux ont permis de déterminer que la GIR doit être intégrée selon deux dimensions : une première dimension transversale (horizontale) permettant de rallier les UF responsables des AGR autour d'une RMC de la problématique de la GIR et de préciser leurs rôles et responsabilités liées à la mitigation des risques (en lien avec les MMC déployées par l'organisation), et une deuxième dimension stratégique (verticale) permettant de fournir un CRC pour les acteurs et leurs actions en créant l'arrimage nécessaire entre les niveaux stratégique, tactique et opérationnel de l'organisation (en lien avec la mission, les objectifs et les opérations de l'organisation). Finalement, des outils opérationnels concrets (comme les chartes de programmes,

les matrices de gouvernance, les RMC des risques, etc.) ont été produits grâce aux travaux réalisés avec l'organisation partenaire afin d'opérationnaliser les concepts théoriques et de fournir à l'organisation des indicateurs lui permettant d'apprécier les niveaux d'intégration transversale et stratégique de la GIR et d'identifier les éléments précis requérant une amélioration.

Les travaux réalisés dans le cadre du chapitre 7 et l'article *A cooperative structure for integrated risk management in large organizations* ont permis de définir la structure de coopération pour la GIR proposée dans cette thèse ainsi que la manière d'arrimer cette structure à la structure organisationnelle fonctionnelle. Ainsi, en utilisant le concept d'UE, cette structure de coopération permet de consolider l'intégration transversale de la GIR en réunissant dans une même équipe dédiée à la GIR (donc l'ÉGIR) des experts de chacune des UF responsables des AGR ; en utilisant le concept des 3LDD, cette structure de coopération permet de consolider l'intégration stratégique de la GIR en créant l'arrimage requis entre les niveaux stratégique, tactique et opérationnel de l'organisation. Au niveau de l'arrimage de la structure de coopération à la structure organisationnelle fonctionnelle, les travaux réalisés avec l'organisation partenaire ont permis de vérifier que la structure matricielle (faible) n'était pas adaptée à la GIR. En raison de l'ampleur de la tâche à réaliser, les personnes qui font partie de l'ÉGIR ne peuvent assumer d'autres responsabilités en même temps. Par contre, le besoin pour ces personnes de demeurer membres à part entière de leur UF d'origine faisait en sorte qu'une variante de la structure matricielle devait être envisagée. Ainsi, parce qu'elle possède fondamentalement la même structure que la forme matricielle, mais que ses acteurs jouissent en plus d'une plus grande liberté quant à leurs actions et leurs réflexions, la structure agile et organique présente des caractéristiques qui conviennent parfaitement aux initiatives transverses comme la GIR. En définitive, un modèle hybride de la structure matricielle (forte) et de la structure agile et organique a été adopté.

Finalement, la dernière partie des travaux consistait à voir comment un tel cadre de gouvernance pour la GIR pouvait créer de la valeur. Les travaux réalisés dans le cadre du chapitre 8 et l'article *A knowledge-based risk-data aggregation model leveraging social constructivism and shared situational awareness to improve decision-making in large organizations* visaient cet objectif. Le défi consistait alors à déterminer comment les incertitudes sur les risques (donc, sur les différents paramètres du risque, soit les aléas, les impacts et les vulnérabilités) et la perception des acteurs en regard des risques pouvaient être prises en compte par le modèle d'agrégation. Pour intégrer les incertitudes sur les risques, le modèle considère celles-ci comme des facteurs qui accroissent le

risque. Au niveau des indicateurs, les incertitudes sont donc représentées comme des zones de méconnaissances (ou zones grises représentées par des « ? ») et au niveau des calculs, le modèle associe à ces incertitudes une valeur qui correspond au maximum sur l'échelle utilisée par le modèle. Au niveau de l'intégration des perceptions individuelles des acteurs, le modèle mise évidemment sur le développement de l'ISP de ces derniers et, au niveau des calculs, le modèle propose d'objectiver les effets de ces perceptions en utilisant la technique AHP-Delphi. En définitive, la combinaison des indicateurs opérationnels sur l'état des MMC pour les convertir en indicateurs globaux offre une aide à la décision supplémentaire quant à la priorité à donner aux actions visant la mitigation des risques en permettant d'identifier les alignements de vulnérabilités potentiels et les chemins offrant une moindre résistance à la propagation des défaillances, comme il l'a été démontré dans l'article.

Pour conclure cette synthèse des travaux, il est essentiel de revenir sur la question de recherche, qui, à titre de rappel, était la suivante : **Est-il possible de développer un cadre de gouvernance complet et opérationnel pour la GIR qui permettra aux grandes organisations de mieux agréger les ICII sur les risques et de générer des connaissances collectives nouvelles et transdisciplinaires leur permettant de mieux supporter leurs processus de prise de décisions plus tactiques et stratégiques quant aux risques à gérer ?**

La réponse à cette question tient donc en trois temps : (1) le cadre est-il complet ?, (2) le cadre est-il opérationnel ? et (3) le cadre génère-t-il de la valeur ? Au niveau de la complétude du cadre, on peut affirmer que ce cadre est complet en regard de ce qui était visé par cette recherche. Certes, la notion de complétude est quelque peu utopique en ce sens que rien n'est jamais réellement complet. Et, ces travaux et le cadre qu'ils proposent n'ont pas cette prétention. Néanmoins, à l'instar de tout projet, certains critères doivent être établis afin de pouvoir déterminer, au bout du compte, si les objectifs poursuivis ont été atteints ou non. Évidemment, ce cadre n'est pas parfait et d'autres travaux devront être poursuivis afin de venir le complémenter davantage, l'améliorer ou le modifier selon le contexte de son utilisation, mais, globalement, en regard des critères qui avaient été établis, on peut affirmer que ce cadre intègre effectivement les éléments clés de la gouvernance illustrés à la figure 3.3 (et établis grâce à la revue de la littérature du concept de gouvernance) et qu'il couvre aussi la GIR sous ses trois dimensions telles qu'elles ont pu être établies grâce à la revue de la littérature des éléments d'intérêt liés à la GIR (en lien avec les 3 piliers du cadre de gouvernance), à savoir :

1. la dimension gouvernance : en lien avec le partage des rôles et des responsabilités des UF responsables des AGR (via les chartes de programme et les matrices de gouvernance), la documentation du cadre réglementaire de la GIR (via le CRC établi par les politiques, les directives, les processus, les standards/normes, etc.) et l'intégration de la structure de coopération à la structure fonctionnelle. Cette dimension est couverte principalement par les piliers 1 et 2 du cadre de gouvernance.
2. la dimension technique : en lien avec l'identification des vulnérabilités des MMC et la représentation des risques comme des alignements de vulnérabilités potentiels. Cette dimension est couverte principalement par le pilier 3 du cadre de gouvernance.
3. la dimension humaine : en lien avec les enjeux d'incertitude et de perception des risques pris en compte par la capacité des acteurs à développer une connaissance collective transdisciplinaire des risques (principe de socioconstructivisme) et de développer une RMC de ces risques et un COC pour leur gestion (principe d'ISP). Cette dimension est couverte principalement par les piliers 1 et 3 du cadre de gouvernance.

Au niveau de l'opérationnalité du cadre, le travail avec l'organisation partenaire a permis de traduire les concepts théoriques en outils opérationnels concrets utilisables par les grandes organisations suggérant ainsi que celui-ci est effectivement opérationnel, c'est-à-dire que ses concepts ne sont pas uniquement valides en théorie, mais qu'ils sont aussi valides en pratique. Encore ici, il est impossible d'affirmer qu'une organisation pourrait prendre ce cadre et le mettre en place tel quel. D'ailleurs, l'auteur de ces lignes déconseille fortement à quiconque d'essayer d'implémenter ce cadre tel quel dans une autre organisation sans d'abord le comprendre, et sans d'abord analyser comment les caractéristiques particulières propres à l'organisation dans laquelle on voudrait l'implémenter influenceront la constitution de ce cadre. Cependant, la mise en place du cadre dans l'organisation partenaire et les outils qui ont été développés suggèrent qu'il est effectivement opérationnel et qu'il pourrait donc effectivement être adopté par d'autres grandes organisations et adapté pour une utilisation et un contexte propres à elles.

Finalement, au niveau de la création de valeur, le modèle d'agrégation des ICII sur les risques fournit des connaissances nouvelles et transdisciplinaires plus stratégiques capables de mieux supporter les processus de prise de décisions. La capacité du modèle à représenter les risques comme des alignements de vulnérabilités potentiels plutôt que comme le résultat de la probabilité d'occurrence d'un aléa par la somme de ses conséquences change aussi la perspective selon

laquelle les risques sont abordés. Ainsi, plutôt que de mettre l'accent sur l'aléa (élément sur lequel les organisations ont souvent peu de contrôle), l'accent est mis sur la réduction de la vulnérabilité de l'organisation et l'accroissement de sa résilience (par le biais des MMC) et sur la réduction des zones d'incertitudes et de méconnaissances. Ce modèle permet donc autant d'adresser les risques traditionnels que les risques émergents. De plus, la capacité du modèle à identifier les chemins offrant la moindre résistance à la propagation des défaillances (autant du point de vue de la gouvernance entourant le fonctionnement des MMC, donc en lien avec le partage des rôles et des responsabilités des acteurs, que du point de vue de leur état) représente un élément clé de valeur ajoutée qui est recherché de la mise en place de ce cadre de gouvernance, et plus généralement, par la mise en place d'un cadre de GIR. Ainsi, on peut affirmer que la mise en place de ce cadre de gouvernance dans une organisation génère effectivement une valeur qui ne pourrait être autrement générée que par la coopération entre les UF responsables des AGR.

En définitive, et pour conclure cette synthèse, tous ces travaux étaient nécessaires dans le cadre d'une approche rigoureuse qui a effectivement permis d'adapter le concept d'EC pour qu'il prenne la forme du cadre de gouvernance pour la GIR chez les organisations de grande ampleur qui est présenté dans cette thèse.

9.2 Apports scientifiques de la recherche

La synthèse des travaux a permis de confirmer l'atteinte des objectifs de recherche poursuivis. Mais, au-delà de ces objectifs, cette recherche aura aussi permis d'apporter quelques contributions supplémentaires au domaine de la gestion des risques.

Premièrement, cette recherche a permis de préciser la notion de risques émergents. Dans la littérature, le concept de risque émergent revient continuellement, mais il est très difficile de retrouver un seul document qui aborde directement ce concept, qui le met en comparaison directe du concept de risque traditionnel et qui explicite clairement les défis liés à leur gestion, comme il l'a été fait à l'article 2, *Challenges related to emerging risk management*. De plus, la catégorisation des risques émergents en 7 catégories distinctes expliquées et définies est quelque chose qui n'apparaissait pas clairement au niveau de la littérature.

Un autre apport de cette thèse au domaine de la gestion des risques vient de l'analyse du processus de gestion des risques proposé par la norme ISO31000. Ainsi, même si la norme utilise la nouvelle définition du risque qui est basée sur le concept d'incertitude, le processus lui-même n'a pas changé et demeure associé à l'ancienne définition du risque qui, elle, est basée sur son concept mathématique (donc, provenant des sciences exactes). Le processus proposé par la norme semble donc se positionner en porte-à-faux de la nouvelle définition puisqu'il demande encore d'identifier l'aléa et de lui assigner une probabilité d'occurrence. De plus, l'analyse qui a été faite au niveau de l'article 2 ouvre sur une réflexion plus globale quant à la capacité des matrices de risques à pouvoir représenter réalistement les risques émergents et sur la capacité réelle des organisations à pouvoir établir de manière cohérente des seuils de tolérance face à ces risques.

Au niveau de la GIR, cette recherche a permis de positionner la GIR en regard de la gestion des risques. Encore une fois, la GIR est souvent mentionnée dans la littérature. Or, si la plupart du temps l'expression elle-même est bien définie, il semble y avoir un certain décalage au niveau de son application. Ainsi, souvent, au niveau de l'application, on semble sous-entendre que la gestion des risques devient intégrée lorsque toutes les parties prenantes participent au même processus de gestion des risques ou lorsque toutes les parties prenantes font leur gestion des risques chacune de leur côté et que ces résultats sont ensuite mis ensemble. Donc, la GIR est davantage présentée comme un processus de gestion des risques répété à plusieurs reprises et dont les résultats sont rassemblés. Or, non seulement il n'y a pas réellement de valeur ajoutée à une telle approche, puisque le résultat final est alors la somme des résultats individuels, mais une telle approche soulève des doutes quant à la capacité réelle d'une UF responsable d'une AGR de pouvoir conduire un processus de gestion des risques en silo sans avoir idée de l'implication des autres UF. Elle soulève aussi de sérieux doutes quant à la capacité d'assurer la coordination, la complémentarité et la cohérence des décisions et des actions qui sont prises individuellement par ces différents acteurs, puisque les interrelations et les interdépendances entre ceux-ci et entre les risques eux-mêmes ne peuvent alors pas être prises en compte. Au contraire, la GIR comme elle est présentée et définie dans cette thèse fait prendre conscience aux multiples parties prenantes qu'elles n'ont en fait qu'une seule partie de la solution et que la solution elle-même ne peut venir que par la mise en commun de toutes ces parties de solution, comme le sont les pièces d'un casse-tête (le résultat final est alors plus grand que la somme des résultats individuels). Au niveau de l'apport scientifique, cela

représente un positionnement majeur de la GIR en tant qu'activité hautement stratégique à bien plus forte valeur ajoutée.

Un autre apport de ces travaux de recherche au domaine de la gestion des risques est la manière dont la perception des risques est ici abordée. Dans la littérature, la notion de perception des risques est souvent abordée dans son contexte psychologique. C'est très bien et cela doit être fait, mais pour une organisation, aborder la perception des risques sous cet angle est difficilement exploitable. Ainsi, dans cette thèse, les effets des perceptions individuelles des acteurs sont davantage associés à des incertitudes accroissant le risque. Pour réduire les effets de ces perceptions, les travaux misent sur l'accroissement de la connaissance collective transdisciplinaire sur les risques et le développement de l'ISP de ces acteurs. L'utilisation de la technique AHP-Delphi, comme outil permettant d'objectiver les effets des perceptions individuelles des acteurs en permettant leur intégration au niveau des calculs des indices de risques, représente une manière concrète pour les organisations d'intégrer ces effets dans les calculs et, au bout du compte, d'obtenir une forme de consensus organisationnel de la valeur d'un risque par rapport à un autre, donc une priorisation des risques qui tienne compte des perceptions individuelles des acteurs. Certes, rien de tout cela n'est parfait et d'autres travaux seront requis pour mieux définir, comprendre et consolider cet aspect du cadre, mais il s'agit certainement d'une manière intéressante de considérer cette variable dans les analyses de risques et qui mérite d'être explorée davantage.

Finalement, un autre apport de cette thèse est qu'il est désormais possible de parvenir à identifier et mesurer les alignements de vulnérabilité potentiels et les chemins offrant une moindre résistance à la propagation des défaillances. Dans l'article 2 sur les défis liés à la gestion des risques émergents, on mentionne que ces risques sont davantage le résultat d'une suite d'événements fortuits ayant conduit à une défaillance. Dans la méthodologie de recherche, on mentionne que la plupart des accidents sont expliqués *a posteriori* puisque les enquêtes arrivent dans la grande majorité des cas à recréer la séquence des événements (défaillances) ayant conduit à l'accident. Comme il l'est mentionné à la section 4.1 : « « les astres étaient alignés pour que ça arrive »… mais encore fallait-il avoir les moyens d'observer, voire de mesurer, cet alignement ». Or, ce qui ressort des travaux présentés dans cette thèse, c'est qu'il est possible d'identifier ces alignements de vulnérabilités avant qu'ils ne surviennent grâce aux RMC des risques comme celle illustrée à la figure 8.4. Comme DOMINO, cette approche permet alors de faire des analyses basées sur des scénarios quelconques et ouvre directement la voie à la possibilité d'utiliser des algorithmes

informatiques ou des systèmes basés sur l'IA afin de bénéficier des capacités de traitement de ces outils. De tels outils pourraient non seulement permettre d'accélérer le traitement des ICII sur les risques, mais pourraient aussi faire en sorte que des analyses de type *rétro-ingénierie*[37] des risques soient réalisées : en faisant varier les états des MMC afin de représenter des états futurs possibles générant des défaillances, ces outils pourraient prédire des situations de risque potentielles avant même qu'elles ne surviennent et ainsi aider à la conception de systèmes résilients par design[38]. L'approche présentée dans cette thèse ouvre cette possibilité qui constituerait une avancée intéressante dans le domaine de la gestion des risques.

9.3 Limites de la recherche et perspectives de projets

Bien qu'ils aient permis d'atteindre les objectifs poursuivis et malgré les apports scientifiques, ces travaux de recherche présentent toutefois quelques limitations qui doivent être mentionnées. De l'avis de l'auteur de ces lignes, ces limitations ne remettent pas en question la valeur scientifique de cette thèse pour le domaine de recherche. Néanmoins, il demeure important de les mentionner puisqu'elles pourraient donner lieu à des travaux qui pourraient être réalisés afin de consolider davantage le cadre de gouvernance développé ou l'adapter à d'autres contextes.

La première limitation de cette recherche est associée au contexte opérationnel dans lequel celle-ci a été conduite. Ce contexte a fait en sorte qu'il y avait une forte volonté (voire, une forme d'obligation) de livrer des résultats concrets pour l'organisation partenaire. Le nombre de ressources engagées dans le projet étant relativement important, clairement un retour sur l'investissement était attendu et tout à fait légitime. Donc, en plus de devoir développer les concepts théoriques sous-tendant les différents éléments du cadre de gouvernance et les traduire sous leur format opérationnel, il fallait aussi livrer chacun de ces éléments. Or, chacun de ces concepts théoriques aurait très bien pu faire l'objet d'une thèse. La coopération, la gouvernance, les risques

[37] La rétro-ingénierie ou ingénierie inversée (ou *reverse-engineering*, en anglais), est « le processus de désassemblage et d'analyse d'un produit fini visant à découvrir comment il fonctionne, à recréer ou à améliorer des éléments obsolètes ou rares, ou à stimuler l'innovation » (Autodesk.com, 2025). Appliqué au domaine des risques et dans le contexte présenté dans cette thèse, ce concept pourrait permettre de comprendre la dynamique du fonctionnement et de la propagation des risques sur les chemins offrant un alignement de vulnérabilités afin de mettre en place des MMC spécifiques (un fonctionnement similaire à la méthode de l'arbre des causes, mais qui au lieu de considérer la défaillance d'une MMC, prendrait plutôt en compte ses vulnérabilités).

[38] La résilience par design (ou *resilience by design*, en anglais), est une approche stratégique axée sur la création de systèmes et de stratégies capables de continuer à opérer, de s'adapter et de se rétablir efficacement face aux perturbations. Elle implique l'intégration des principes de résilience dans la conception de divers aspects d'une entreprise ou d'une organisation, tels que les personnes, les processus, les stratégies et les systèmes (Schnewlin, 2024).

émergents, le socioconstructivisme, l'intelligence situationnelle partagée, la perception des risques, etc. Or, découlant du contexte, et dans un souci de livrer des résultats intéressants et tangibles pour l'organisation partenaire, il n'a certainement pas été possible d'aller dans le fin détail de tous ces concepts. Néanmoins, à chaque fois qu'il l'a été jugé nécessaire, un effort a été réalisé afin d'aborder assez en profondeur ces concepts pour en retirer les apprentissages pertinents au développement du cadre de gouvernance proposé dans cette thèse et afin de permettre au lecteur de suivre le raisonnement du chercheur à chaque étape du processus de recherche. Cette limitation ouvre cependant la voie vers d'autres travaux plus ciblés afin de consolider davantage les différents éléments du cadre de gouvernance proposé.

Une autre limitation de cette recherche est associée à la portée des travaux. L'objectif ultime recherché par le cadre de gouvernance pour la GIR chez les organisations de grande ampleur proposé dans cette thèse est de pouvoir intégrer l'ensemble des risques organisationnels à l'intérieur d'un même référentiel. Or, dans son volet pratique (donc au niveau de l'organisation partenaire), ce projet de recherche se voulait un projet-pilote permettant de développer un cadre de gouvernance pour la GIR et de démontrer la pertinence et la valeur ajoutée de la mise en place d'un tel cadre. Ainsi, dans son volet pratique, cette recherche a été limitée à la direction « Sûreté et résilience de l'entreprise » de l'organisation partenaire, qui regroupe 4 UF responsables de : (1) la continuité des affaires, (2) la gestion des accès, (3) la gestion des incidents et des mesures d'urgence et (4) la protection des actifs et la sécurité physique. Si le projet-pilote était jugé concluant, alors une représentation au niveau de la vice-présidence « Responsabilités corporatives et risques » allait être faite afin d'élargir le projet aux autres UF sous cette vice-présidence. Ces UF sont réparties dans 5 autres directions : (1) les assurances, (2) l'environnement, (3) la prévention des pertes, la fraude et les enquêtes, (4) la santé et la sécurité au travail et (5) la sécurité de l'information et la sécurité informatique. Ainsi, pour réellement prendre la mesure de l'envergure de ce projet, si celui-ci avait intégré l'ensemble des UF responsables des AGR chez l'organisation partenaire, il aurait fallu intégrer les 9 UF sous la vice-présidence « Responsabilités corporatives et risques ». Une question se pose alors : le résultat final aurait-il été différent si toutes ces UF avaient participé au projet ? Donc, la question est à savoir si la participation au projet d'autres personnes, avec d'autres connaissances, compétences et expertises, aurait eu pour effet d'enligner les travaux dans une autre direction avec pour résultat final, un cadre de gouvernance différent de celui obtenu. Cela est très difficile à déterminer, néanmoins, le fait que le cadre ait été développé sur la base des

concepts existants de l'EC et sur la base de concepts théoriques qui ont ensuite été opérationnalisés sous la forme d'outils, porte à croire que non. Cependant, bien qu'il soit impossible de répondre avec certitude à ce questionnement, cette limitation ouvre la voie vers un élargissement du projet-pilote aux autres UF responsables des AGR chez l'organisation partenaire. Les étapes subséquentes seront donc de présenter les résultats de ce projet de recherche au niveau de la vice-présidence « Responsabilités corporatives et risques » afin de mesurer l'intérêt à élargir la portée du cadre de gouvernance aux autres UF sous cette vice-présidence, ce qui pourrait donner lieu à un projet à l'interne de l'organisation partenaire qui pourrait venir complémenter ces travaux et bonifier le cadre de gouvernance en y intégrant des connaissances et des expertises nouvelles.

Une autre limitation de cette recherche concerne le balisage. En effet, comme le projet de recherche se faisait dans une organisation spécifique et en réponse à une problématique spécifique observée par le chercheur au sein de l'organisation partenaire, il n'était pas dans les objectifs du projet de conduire un balisage auprès d'autres grandes organisations québécoises, canadiennes ou autres, pour voir comment celles-ci abordent la GIR. Ainsi, une hypothèse a été faite par le chercheur dès le début des travaux et celle-ci aurait pu (ou a peut-être) générer un biais cognitif au niveau du raisonnement du chercheur (dans ce cas-ci, un biais de confirmation[39]). Cette hypothèse tient du fait que l'organisation partenaire est une grande organisation canadienne (la plus grande de son secteur d'activités), qu'elle possède une très longue histoire, une très grande équipe responsable de gérer les risques et qui investit considérablement dans la gestion des risques. Basé sur ces éléments, il a été pris pour acquis que si cette organisation vit une certaine problématique au niveau de la GIR, il y a fort à parier que plusieurs autres grandes organisations vivent exactement la même problématique. Or, cela n'a pas été directement prouvé dans le cadre de cette thèse. Plutôt, il en a été déduit par la rétrospective du projet DOMINO qui a impliqué plusieurs très grandes organisations du Québec, par les travaux de Jean-Jules et Vicente (2020) qui ont montré que plusieurs grandes organisations n'arrivent pas à mettre en place la GIR malgré les ressources qu'elles y investissent et par l'analyse des éléments d'intérêt disponibles aux grandes organisations lors de la revue de la littérature, qu'il y avait un certain manque dans la littérature au niveau de la gouvernance associée à la GIR chez les organisations de grande ampleur. Ainsi, même en étant

[39] Un biais de confirmation (ou biais de confirmation d'hypothèse) est une « tendance, souvent inconsciente, à être trop favorable envers les informations qui confirment une hypothèse, et ce, au détriment de celles qui la contredisent » (Guide pratique des biais cognitifs.com, 2025).

largement confiant que cette problématique est bien réelle, il serait intéressant de conduire un balisage en bonne et due forme auprès d'autres grandes organisations du Québec, du Canada ou ailleurs pour voir comment celles-ci abordent la GIR. Une telle initiative permettrait d'évaluer et de déterminer de manière plus exhaustive dans quelle mesure cette problématique est répandue au sein de ces grandes organisations et ainsi, avoir une idée plus précise de l'apport de ce cadre de gouvernance pour la GIR pour les grandes organisations. De tels travaux pourraient aussi permettre de bonifier le cadre développé en s'inspirant de diverses façons de faire et des meilleures pratiques.

Une autre limitation de cette recherche concerne la réplicabilité. Ici, on entend la réplicabilité de l'implémentation du cadre de gouvernance pour la GIR dans une autre organisation et non la réplicabilité de la recherche elle-même. En effet, tout au long de ces travaux, un souci particulier a été apporté afin de faire en sorte que le cadre de gouvernance développé soit assez général et simple pour pouvoir être implémenté chez d'autres grandes organisations. L'idée étant qu'une grande organisation quelconque pourrait prendre ce cadre et l'appliquer à l'interne avec, évidemment, l'adaptation requise, d'où l'intérêt de conduire ce projet avec une organisation partenaire. Or, la réalité est que l'intervention du chercheur a été considérable tout au long du projet, même par rapport à son volet pratique, si bien qu'il demeure difficile d'évaluer si ce cadre est effectivement aussi facile à implémenter dans une autre grande organisation sans intervention externe d'une personne possédant des compétences assez fines dans le domaine de la gestion des risques pour bien comprendre ce qui va fonctionner et ce qui ne va pas fonctionner et, surtout, pour pouvoir juger de la validité des résultats obtenus. Ainsi, pour vérifier si le cadre proposé dans cette thèse est facilement réplicable au niveau d'autres grandes organisations, il faudrait que l'une de ces grandes organisations (ou plusieurs) soit disposée à mettre en place ce cadre de gouvernance pour la GIR, mais cette fois, avec peu d'intervention externe d'un chercheur. Cela permettrait de savoir dans quelle mesure la mise en place de ce cadre de gouvernance est facile pour une organisation à l'extérieur d'un cadre de recherche et ouvrirait aussi la voie à l'amélioration du cadre de gouvernance développé et, possiblement, si un tel projet venait à en démontrer la pertinence (voire, la nécessité), au développement d'outils d'accompagnement tels que des formations, des guides méthodologiques, ou des séances de consultation. La rétroaction d'un tel projet pourrait aussi permettre d'identifier des critères spécifiques permettant de déterminer, par exemple, à partir de quand une organisation est considérée d'une ampleur assez grande pour que ce cadre de gouvernance trouve sa pertinence. Est-ce à partir d'un certain nombre d'unités d'affaires, d'un

certain nombre d'UF responsables des AGR ou d'un certain nombre d'employés ? Ou d'autres critères doivent-ils être considérés ou sont-ils plus pertinents ? Un tel travail pourrait également permettre de développer des variantes du cadre de gouvernance applicables à des organisations de natures différentes (par exemple, des municipalités ou des organismes gouvernementaux) ou à des organisations de plus petite dimension, comme les petites et moyennes entreprises, c'est-à-dire celles qui emploient moins de 500 employés. Il serait d'ailleurs très intéressant d'explorer cette avenue sachant que l'activité économique dépend largement de la contribution de ces entreprises[40].

Finalement, une autre limitation de cette recherche concerne la pérennité du cadre de gouvernance. En effet, l'une des grandes conclusions issues de la rétrospective du projet DOMINO concernait la difficulté de maintenir dans le temps un EC dédié aux risques. Ainsi, dans le cadre de ces travaux, l'avenue qui a été envisagée pour régler cette situation était d'ancrer la structure de coopération liée à la GIR directement à la structure organisationnelle. Or, à la fin du projet de recherche, une restructuration majeure a eu lieu au sein de l'organisation partenaire qui a fait en sorte que la direction « Sûreté et résilience de l'entreprise » a été dissoute et ses UF ont été réparties sous des directions différentes. Par le fait même, le projet faisant l'objet de ces travaux de recherche n'a pas été reconduit. Cette situation, bien que désolante au niveau des perspectives que ce projet ouvrait pour l'organisation partenaire, soulève toutefois une question majeure : comment un tel cadre peut-il survivre à ces restructurations majeures qui arrivent périodiquement au sein des grandes organisations ? Malheureusement, ce projet de recherche n'a pas permis de répondre à cette question. Néanmoins, cette situation démontre que l'avenue qui avait été envisagée dans le cadre de ces travaux de recherche, c'est-à-dire d'ancrer la structure de coopération à la structure organisationnelle, n'est pas suffisante puisqu'elle ne permet pas de résoudre cet enjeu des restructurations qui viennent changer la structure même de l'organisation. Ainsi, de nouvelles pistes de réflexion doivent être explorées. L'une d'elles est certainement le fait que la GIR doit absolument être une priorité absolue de la très haute direction de l'organisation et de son conseil d'administration. Si la GIR demeure l'initiative d'une seule direction ou de quelques acteurs dans l'organisation, mais qu'elle n'est pas soutenue aux plus hauts niveaux organisationnels, alors elle

[40] Au Canada, une entreprise est considérée petite si elle compte moins de 100 employés, elle est considéré moyenne si elle compte entre 100 et 499 employés et elle est considérée grande si elle compte 500 employés et plus. Les petites et moyennes entreprises (PME) sont donc celles qui emploient 499 employés ou moins. Selon les statistiques de 2023, ces entreprises contribuaient à plus de 48,2% du produit intérieur brut Canadien et employaient quelques 9,5 millions de personnes au Canada, soit près de 53,8% de l'emploi total (Innovation, Sciences et Développement économique Canada, 2023).

sera tôt ou tard vouée à disparaître au gré des restructurations ou de la rotation du personnel. Une autre avenue intéressante pourrait être d'intégrer les bonnes pratiques liées à la GIR directement au niveau des normes et des standards liés à la gestion des risques (par exemple, en ayant un standard dans la famille des standards ISO31000 qui soit dédié à la GIR), mais aussi au niveau des normes et des standards liés à la gestion des actifs (famille des standards ISO55000) (Komljenovic et al., 2016). En effet, comme les organisations s'appuient pour la plupart sur des standards établis afin de les guider dans leurs pratiques, cette manière de procéder pourrait rendre la GIR moins tributaire des changements organisationnels. De plus, cela pourrait faire en sorte que la GIR devienne partie intégrante de la gestion des actifs. Comme il l'a été montré dans cette thèse, et comme le suggère aussi l'IRGC (2017), la gestion des risques émergents demande de travailler au niveau de la réduction de la vulnérabilité des organisations et l'accroissement de leur résilience (IRGC 2017 ; Komljenovic et al., 2016). Or, si on accepte le concept de risque proposé dans cette thèse (i.e. le modèle d'agrégation), la vulnérabilité et la résilience d'une organisation sont directement reliées aux actifs et à l'état des MMC qui sont mises en place par l'organisation pour protéger ses actifs ou les rétablir après une défaillance. Il serait donc très intéressant d'explorer cette avenue et de voir comment les apprentissages effectués au cours de ces travaux de recherche (et les outils proposés) pourraient être intégrés à ces standards liés à la gestion des actifs.

Plus généralement, ces travaux de recherche, mais surtout les travaux qui ont été conduits avec l'organisation partenaire, corroborent les difficultés soulevées par la littérature quant à la prise en compte des perceptions individuelles des acteurs dans les analyses de risques. En effet, comme il l'a été expliqué au chapitre 8, la perception à une incidence directe sur le jugement et influence indubitablement la prise de décisions, surtout dans un contexte d'incertitude. Et, comme la perception est spécifique à chaque individu et qu'elle varie selon plusieurs facteurs et selon le contexte, elle a une incidence directe sur la manière dont les individus gèrent les risques. Or, cet enjeu de la prise en compte des perceptions individuelles des acteurs dans la gestion des risques est d'autant plus important dans le contexte des grandes organisations puisque celles-ci sont composées d'une multitude d'individus (d'acteurs) et que ceux-ci jouent un rôle déterminant dans la gestion des risques. Ainsi, si un acteur a tendance à sous-estimer les risques, il aura forcément tendance à en minimiser la gestion pouvant mettre l'organisation devant des situations problématiques. Le contraire est aussi vrai. Si un acteur a tendance à surestimer les risques, il pourrait faire perdre à l'organisation des opportunités d'affaires, lui engendrer des coûts

supplémentaires inutiles au niveau de la mise en place de MMC pour réduire un risque surévalué ou nuire à la prise de décisions quant à la priorisation des risques à gérer. Ainsi, une organisation, qui est une personne morale en soi, ne peut fonder sa stratégie de gestion des risques et ses prises de décisions relatives aux risques sur la base des perceptions qu'en ont individuellement les acteurs qui la composent, même si, au bout du compte, ce sont ces mêmes acteurs qui prennent les décisions en regard de la mitigation des risques au nom de l'organisation. Cet enjeu de la prise en compte des perceptions individuelles des acteurs est donc majeur dans un contexte organisationnel et dans un contexte de GIR. Et, bien que les travaux présentés dans cette thèse proposent une certaine approche pour intégrer les effets des perceptions individuelles des acteurs dans les analyses de risques, force est d'admettre que cette approche est très préliminaire et que des travaux beaucoup plus ciblés devront être entrepris pour mieux comprendre les facteurs qui influencent la perception des risques chez les acteurs, mais aussi, et surtout, pour mieux comprendre comment cette perception influence la dynamique des relations entre les acteurs et la dynamique de prise de décisions en regard des risques, surtout dans le contexte organisationnel spécifique aux grandes organisations.

Ainsi, toutes ces limitations ouvrent la voie vers des perspectives de projets qui permettront de consolider davantage le cadre de gouvernance proposé dans cette thèse ou en développer de nouvelles variantes adaptées à d'autres contextes et, de manière plus générale, accroître la connaissance collective dans les domaines de la gestion des risques et de la GIR.

CHAPITRE 10 CONCLUSION

La division du travail en fonctions est largement prédominante dans les grandes organisations. Si cette manière de procéder est très efficace pour adresser les opérations courantes et permet de répondre adéquatement à certaines problématiques précises, elle atteint ses limites lorsqu'il est question d'aborder les problématiques transverses, c'est-à-dire les problématiques qui transcendent les frontières des silos organisationnels et les frontières des connaissances et qui affectent toute l'organisation. Pour gérer ces problématiques plus efficacement, des approches intégrées et multidisciplinaires, qui impliquent l'ensemble des parties prenantes concernées, sont nécessaires. Or, lorsque plusieurs parties prenantes sont impliquées dans la même entreprise, une solide gouvernance doit être établie afin de s'assurer que chacune d'elles comprenne bien ses rôles et ses responsabilités (et celles des autres) dans l'entreprise commune, et surtout, afin de s'assurer de la coordination, la complémentarité et la cohérence de leurs décisions et de leurs actions.

La GIR est l'une de ces problématiques transverses qui requièrent la mise en place d'une gouvernance qui lui soit spécifique. Et, les travaux présentés dans cette thèse ont permis de formaliser un cadre de gouvernance pour la GIR chez les organisations de grande ampleur. Contrairement à la plupart des cadres existants, qui ressemblent davantage à des processus de gestion des risques auxquels des éléments de gouvernance ont été greffés, celui présenté dans cette thèse a directement été conçu autour du concept de gouvernance et spécifiquement pour la GIR. De plus, contrairement aux cadres existants dont la plupart reposent sur le concept de risque traditionnel, c'est-à-dire qui tend à représenter le risque sous son concept mathématique (reposant sur les sciences exactes), celui présenté dans cette thèse repose sur le concept de risque basé sur l'incertitude, davantage en adéquation avec les caractéristiques des risques émergents. Dans cette optique, réduire le risque ne revient plus à réduire la probabilité d'occurrence d'un aléa (paramètre sur lequel l'organisation a souvent bien peu de contrôle), mais plutôt à accroître la connaissance collective et la compréhension de l'organisation des risques auxquels elle est confrontée. Le raisonnement derrière l'approche : si le risque naît de l'incertitude et que l'incertitude naît du manque de connaissance, alors réduire le risque demande de réduire l'incertitude, donc, d'augmenter la connaissance. De quelles connaissances parle-t-on ? Des connaissances sur le

fonctionnement des systèmes (des actifs), sur leurs vulnérabilités et leur résilience, sur les impacts de leurs défaillances et sur les environnements dans lesquels ces systèmes (ces actifs) évoluent.

La mise en place du cadre proposé à l'intérieur de l'organisation partenaire a permis de développer un cadre de gouvernance qui est valide autant théoriquement, que pratiquement. Ainsi, pour chacun des piliers du cadre de gouvernance, le volet théorique du projet a permis d'établir les concepts à la base de celui-ci, alors que le volet pratique a permis de trouver une manière d'opérationnaliser ces concepts en les traduisant en outils utilisables par les organisations (comme les chartes de programmes, les matrices de gouvernance, les RMC des risques, etc.). Au bout du compte, le cadre développé, non seulement répond relativement bien aux besoins qui avaient été identifiés chez l'organisation partenaire, mais il est aussi assez général, suggérant qu'il pourrait être utilisé par d'autres grandes organisations.

Néanmoins, la mise en place d'un tel cadre de gouvernance pour la GIR dans une organisation ne sera pas aussi facile si l'organisation n'est pas prête à revoir ses façons de faire. Elle doit s'inscrire dans une réelle volonté de changement de culture organisationnelle passant d'une structure de travail en silo (où chaque UF est davantage centrée sur elle-même) vers un modèle où chacune d'elle travaille dans un dessein commun. Ce changement de perspective peut sembler anodin, mais dans les faits, il est majeur. Pour cette raison, plusieurs étapes préliminaires sont nécessaires avant de se lancer dans une telle entreprise. D'abord, il s'agit de fédérer tous les acteurs concernés autour de la cause commune (la GIR), mais il s'agit aussi de clairement établir les objectifs et les attentes spécifiques à chacun de ces acteurs et ceux de l'organisation. Ensuite, chacun des piliers du cadre doit être adapté à la réalité de l'organisation, que ce soit au niveau du référentiel commun, de la structure de coopération ou du modèle d'agrégation des ICII sur les risques. Cette adaptation est nécessaire et peut demander un travail considérable. Pour cette raison, toute organisation qui désirerait mettre en place ce cadre de gouvernance doit d'abord et avant tout le comprendre. Et, le mandat de cette mise en place ne peut être donné qu'à des personnes ayant les connaissances et les compétences requises pour le faire.

Par ailleurs, une fois mis en place, ce cadre demande aussi un certain temps (période de rodage) avant de réellement porter ses fruits. La patience est donc de mise. Pour cela, le support de la haute direction et le maintien de l'intérêt des acteurs impliqués deviennent des conditions *sine qua non* à la réussite d'une telle initiative. Or, une fois les premiers résultats établis, la valeur ajoutée de la

GIR ne fait aucun doute. À une ère où le bon fonctionnement de la société repose très largement sur le bon fonctionnement de ses grandes institutions et corporations, celles-ci ont un devoir moral d'assurer la résilience de leurs opérations. Il devient donc absolument impératif pour ces grandes organisations d'adopter de solides pratiques de saine gouvernance relativement à la manière dont elles gèrent les risques et de mettre la GIR au coeur de leurs priorités.

Pour conclure, j'ai commencé cette thèse en partant des travaux sur DOMINO et en mentionnant que ceux-ci étaient en avance sur leur temps. Je le pense vraiment. Devant l'ampleur des défis liés à la gestion des risques émergents, force est de constater que la GIR prise de manière individuelle, organisation par organisation, comme elle est présentée dans cette thèse, n'est pas suffisante pour adresser la complexité croissante de ces risques et ne sera définitivement pas suffisante pour adresser les risques émergents de demain. Néanmoins, s'inscrivant dans un processus d'accroissement de la maturité des organisations en regard de la manière dont elles gèrent les risques, celle-ci est pratiquement un passage obligé vers des approches multiorganisationnelles de GIR. Les grands défis qui attendent les générations futures méritent des approches nouvelles permettant de combiner des informations de diverses natures et provenant de diverses sources. Surtout, il s'agit de faire en sorte que les informations soient bonnes, soient bien agrégées et corrélées, soient remises entre les bonnes mains, au bon moment, et génèrent les bonnes actions. Ainsi, s'inscrivant dans un souci d'amélioration continue, les résultats des travaux présentés dans cette thèse ne constituent absolument pas une fin en soi, mais plutôt une contribution supplémentaire vers des approches de GIR plus efficaces et consolidées. Si la Crise du verglas de 1998 a été l'élément déclencheur d'une prise de conscience collective des interdépendances au Québec et que les attentats terroristes sur le World Trade Center de New York en 2001 leur ont donné une perspective mondiale, les événements sociaux, sanitaires, climatiques et géopolitiques que nous vivons depuis quelques années déjà sont des exemples éloquents que les risques émergents demandent une réponse globale. Pour DOMINO, j'ose croire que ce n'est donc que partie remise.

RÉFÉRENCES

Adams, P. (2006). “Exploring social constructivism: Theories and practicalities”, *Education 3-13*, Vol. 34, No. 3, pp.243–257.

Agaisse, J.-P., Binhas. L., Bisson, M., Dancause, L., Desbois, A. O., Dourthe, M., Evoy, L., Fortin, A., Garrow, S., Grenier, P., Gruet, É., Bouchard, M. J., Jézéquel, M., Lagacé, M. C., Lefebvre, S., Lemire, N., Manceau, M. et Plant, B. (2018). “Guide pratique sur l’impact”, CommunAgir, [En ligne] https://chantier.qc.ca/wp-content/uploads/2018/05/guide_pratique_impact_2018.pdf, Page consultée le 8 mars 2025.

Amansou, S. (2019). “Le rôle de l’acteur dans la gestion intégrée des risques : vers un nouveau dimensionnement du risque”, Revue du contrôle, de la comptabilité et de l’audit, Vol. 3, No. 4, pp. 932–956.

Amansou, S. et Chaouki, F. (2019). “Essai de délimitation conceptuelle de la gestion intégrée des risques”, Revue du contrôle, de la comptabilité et de l’audit”, Numéro 9 : Décembre 2019 / Vol. 4, No. 3, pp. 357–375.

AMF (2015). *Ligne directrice sur la gestion intégrée des risques*, [En ligne] https://lautorite.qc.ca/fileadmin/lautorite/reglementation/lignes-directrices-toutes-institutions/LD_gestion-integree-risques_fr.pdf, Page consultée ele 15 octobre 2024.

AMF (2021). *Ligne directrice sur la gouvernance*, [En ligne] https://lautorite.qc.ca/fileadmin/lautorite/reglementation/lignes-directrices-toutes-institutions/ligne-directrice-gouvernance_fr.pdf, Page consultée ele 15 octobre 2024.

Amin, M. (2002). “Modelling and control of complex interactive networks”, *IEEE Control Systems Magazine*, Vol. 22, Issue 1, pp. 22-27.

Arena, M., Arnaboldi, M. et Azzone, G. (2010). “The organizational dynamics of enterprise risk management”, Accounting, Organizations and Society, Vol. 35, pp. 659–675.Amin, M. (2002), “Modelling and control of complex interactive networks”, *IEEE Control Systems Magazine*, Vol. 22, Issue 1, pp. 22–27.

Arnoux, J. (2015). “Les défis du partage d’informations entre des fournisseurs de services de télécommunication interdépendants”, Master’s thesis, Polytechnique Montréal.

Bagherigorji, R., Nourtaghani, A., et Farrokhzad, M. (2022). “Multicriteria Decision-Making Model for the Selection of an Affordable Prefabricated Housing System Using Delphi-AHP Method”, *Journal of Architectural Engineering*, Vol. 28 No. 3, [En ligne] https://doi.org/10.1061/(ASCE)AE.1943-5568.0000545, Page consultée le 11 novembre 2023.

Baker, P.R. et Benny, D.J. (2014). The Complete Guide to Physical Security. Auerbach Publications, 360 pages.

Banque des règlements internationaux (2012). *Principes fondamentaux pour un contrôle bancaire efficace*, Comité de Bâle sur le contrôle bancaire, Bank for international settlements, Basel Committee on Banking Supervision, Joint Forum, Principles for the supervision of financial conglomerates, September 2012.

Barnett, J. et Breakwell, G. M. (2001). “Risk perception and experience: Hazard personality profiles and individual differences”, *Risk Analysis*, Vol. 21 No. 1, pp. 171–178.

Basel Committee on Banking Supervision (2012). “Principles for effective risk data aggregation and risk reporting”, [En ligne] https://www.bis.org/publ/bcbs222.pdf, Page consultée le 20 septembre 2023.

Beghetto, R. A. (2021). “There is no creativity without uncertainty: Dubito ergo creo”, *Journal of Creativity*, Vol. 31, [En ligne] https://doi.org/10.1016/j.yjoc.2021.100005, Page consultée le 22 novembre 2023.

Bernoulli, D. (1738). “Spécimen Theoriae Novae de Mensura Sortis”, Proceedings of the Impérial Academy, Vol. 5, pp. 175–192.

Bharosa, N., Lee, J., et Janssen, M. (2010). “Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises”, *Information Systems Frontiers*, Vol. 12, Issue 1, pp. 49–65.

Bohnert, A., Gatzert, N., Hoyt, R. E. et Lechner, P. (2019). “The drivers and value of enterprise risk management: Evidence from ERM ratings”, *The European Journal of Finance*, Vol. 29 No. 5, pp. 234–255.

Boivin, S., Leyrie, C. et Boigey, P. (2022). Pour des parties prenantes engagées dans les projets : réflexions théoriques et pratiques, Presses de l'Université du Québec, 250 pages.

Brouillette, X. (2009). "Platon, précurseur de la "saine gouvernance"? Les idées gestionnaires à la mode nous ramènent en partie à la position platonicienne où des experts doivent avoir le pouvoir", *Le Devoir*, November 14–15, 2009, page C-6.

Business Lab (2022). Quels sont les actifs tangibles et les actifs intangibles d'une entreprise, [En ligne] https://www.businesslab.fr/quels-sont-les-actifs-tangibles-et-les-actifs-intangibles-d-une-entreprise/, Page consultée le 21 décembre 2023.

Canadian Encyclopedia (2014). Public policy, [En ligne] https://www.thecanadianencyclopedia.ca/en/article/public-policy, Page consultée le 16 mai 2023.

Caron, D. J., Bherer, A. et Bernardi, S. (2020). "La gouvernance informationnelle au sein de l'administration publique", Chaire de recherche en exploitation des ressources informationnelles, École Nationale d'Administration Publique, Mars 2020, 51 pages, [En ligne] https://espace.enap.ca/id/eprint/318/1/Caron%2C%20DanielJ_Gouvernance_20220107.pdf, Page consultée le 19 janvier 2023.

CCPS (2018). Bow Ties in Risk Management: A Concept Book for Process Safety, 1st ed, Center for Chemical Process Safety (CCPS), Wiley-AlChe, 224 pages.

CDSE (2017). Introduction to Physical Security: Student Guide, Center for Development of Security Excellence, [En ligne] https://www.cdse.edu/Portals/124/Documents/student-guides/PY011-guide.pdf, Page consultée le 17 mars 2024.

Chen, J., Sohal, A.S. and Prajogo, D.I. (2013). "Supply chain operational risk mitigation: a collaborative approach", *International Journal or Production*, Vol. 51, No. 7, pp. 2186–2199.

Chionis, D., Karanikas, N., Iordan, A. R. et Svensson-Dianellou, A. (2022). "Risk perception and communication factors in aviation: Insights from safety investigators", *Journal of Risk Research*, Vol. 25, No. 7, pp. 844–859.

Cho, G. (2005). *Geographic information science: Mastering the legal issues*, New York: John Wiley and Sons.

Cisternas, P. C., Cifuentes, L. A., Bronfman, N. C., et Repetto, P. B. (2023). “The influence of risk awareness and government trust on risk perception and preparedness for natural hazards”, *Risk Analysis*, [En ligne] https://doi.org/10.1111/risa.14151, Page consultée le 6 juin 2024.

Cook, L., et Friend, M. (1991). “Principles for the practice of collaboration in schools”, *Preventing School Failures*, Vol. 35, Issue 4, pp. 6–9.

COSO (2004). *Enterprise Risk Management Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission (COSO), [En ligne] https://www.coso.org/_files/ugd/3059fc_ae81f45d98474c9188045cbacbd510bf.pdf, Page consultée le 30 novembre 2023.

COSO (2017). *Enterprise Risk Management: Integrating with Strategy and Performance*, Committee of Sponsoring Organizations of the Treadway Commission (COSO), [En ligne] https://www.coso.org/, Page consultée le 11 février 2023.

CRP (2013). *Rapport sur les infrastructures critiques localisées à l’intérieur des secteurs alimentés par les conduites d’eau à réhabilitées à Montréal*, Centre risque & performance, Polytechnique Montréal.

Cutter, S.L. (2003). “GI science, disasters, and emergency management”, *Transactions in GIS*, Vol. 7, Issue 4, pp. 439–445.

Davel, E., et Tremblay, D.-G. (2006). “Communauté de pratique : Défis et pratiques contemporaines”, Université du Québec à Montréal, [En ligne] http://recitsrecettes.org/sites/default/files/davel_ettremblay_communautes_prat.pdf, Page consultée le 3 mai 2021.

Delvosalle, C., Robert, B., Nourry, J., Brohez, S., et Yan, G. (2017). “Considering critical infrastructures in the land use planning policy around Seveso plants”, *Safety Science*, Vol. 97, pp. 27–33.

Dionne, G. (2013). “Risk management: History, definition and critique”, *Risk Management and Insurance Review*, Vol. 16 No. 2, pp. 147–166.

Dolence, M.G. et Norris, D.M. (1994). “Using key performance indicators to drive strategic decision making”, *New Directions for Institutional Research*, Vol. 1994, No.82, pp. 63–80. [En ligne] https://doi.org/10.1002/ir.37019948207, Page consultée le 4 mars 2024.

Donohue, J. (2023). “IRM vs. ERM: What is the difference and can your organization benefit from both?”, [En ligne] https://www.diligent.com/resources/blog/irm-vs-erm, Page consultée le 16 septembre 2024.

Doran, G. T. (1981). “There's a S.M.A.R.T. way to write management's goals and objectives”, *Management Review*, Vol. 70 No. 11, pp. 35–36.

Doz, Y. L., and Hamel, G. (1998). *Alliance advantage: The art of creating value through partnering*, Cambridge, MA: Harvard Business School Press.

Drucker, P.F. (1954). The Practice of Management, Harper & Row, New York.

Dyer, J. H., et Singh, H. (1998). “The relational view: Cooperative strategy and sources of inter-organizational competitive advantage”, *Academy of Management*, Vol. 23, Issue 4, pp. 660–679.

Edgar, L., Jones Jr, M.D., Harsy, B., Passiment, M., Hauer, K.E. (2021). “Better Decision-Making: Shared Mental Models and the Clinical Competency Committee”, *Journal of Graduate Medical Education*, April 13, 2021, pp.51–58.

Endsley, M. R. (1988). “Design and evaluation for situation awareness enhancement”, *Proceedings of the Human Factors Society Annual Meeting*, Vol. 32 No. 2, pp. 97–101.

Endsley, M. R. (1995). “Toward a theory of situation awareness in dynamic systems”, *Human Factors*, Vol. 37 No. 1, pp. 32–64.

Endsley, M. R. (2015). “Situation Awareness Misconceptions and Misunderstandings”, *Journal of Cognitive Engineering and Decision Making*, Vol. 9, No. 1. pp. 4–32.

ERGEG (2007). “The lessons to be learned from the large disturbance in the European power system on the 4th of November 2006”, European Regulators’ Group for Electricity and Gas, Council of European Energy Regulators ASBL, [En ligne] https://www.ceer.eu/documents/104400/-/-/b4f16360-b355-5d50-bf33-01f8a76fc95a, Page consultée le 4 mai 2021.

European Commission (2016). *Joint Framework on Countering Hybrid Threats: A European Union Response, Joint Communication to the European Parliament and the Council,*

European Commission, April 2016, [En ligne] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018, Page consultée le 22 novembre 2023.

Fernandez, A. (2018). *Les tableaux de bord du manager innovant : une demarche en 7 étapes pour faciliter la prise de décision en équipe*, Paris: Éditions Eyrolles, ISBN: 978-2212569285, 320 pages.

Ferreira, R.S.M., Da Silva, A.P.C., and Murai, F. (2022). "Risk perception and misinformation in Brazilian Twitter during COVID-19 infodemic", in Proceedings - 20th IEEE International Symposium on Parallel and Distributed Processing with Applications, 12th IEEE International Conference on Big Data and Cloud Computing, 12th IEEE International Conference on Sustainable Computing and Communications and 15th IEEE International Conference on Social Computing and Networking, ISPA/BDCloud/SocialCom/SustainCom 2022, pp. 435–442, [En ligne] https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom57177.2022.00062, Page consultée le 21 février 2025.

Frank, A. B., Goud Collins, M., Levin, S. A., Lo, A. W., Ramo, J., Dieckmann, U., Kremenyuk, V., Kryazhimskiy, A., Linnerooth-Bayer, J., Ramalingam, B., Stapleton Roy, J., Saari, D. J., Thurner, S. et Von Winterfeldt, D. (2014). "Dealing with femtorisks in international relations", *Proceedings of the National Academy of Sciences*, Vol. 111 No. 49, pp. 17356–17362.

Gardair, E. (2007). "Heuristiques et biais : quand nos raisonnements ne répondent pas nécessairement aux critères de la pensée scientifique et rationnelle", *Revue électronique de Psychologie Sociale*, 2007, No. 1, pp. 35-46.

Garrido-Pelaz, R., González-Manzano, L. et Pastrana, S. (2016). "Shall we collaborate? A model to analyse the benefits of information sharing", WISCS 2016, *Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security*, co.located with CCS 2016, pp.15–24. [En ligne] https://www.scopus.com/inward/record.uri?eid=2.s2.0.84998698730&doi=10.1145%2f299

4539.2994543&partnerID=40&md5=8100b9ef47dab6e5b815b40c2ad65fcf, Page consultée le 4 août 2022.

Gheorghe, A. V., et Schläpfer, M. (2006). “Ubiquity of digitalization and risks of interdependent critical infrastructures”, *IEEE*, International Conference on Systems, Man, and Cybernetics, Taipei, Taiwan, October 8-11, 2006.

Gilbert, R. B., Habibi, M. et Nadim, F. (2016). “Accounting for unknown unknowns in managing multi-hazard risks”, in Gardoni, P., and LaFave, J. M. (Eds.), *Multi-Hazard Approaches to Civil Infrastructure Engineering*, Springer International Publishing, Cham, Switzerland, pp. 383–412.

Gooding, H., Lattanzio, S., Newnes, L., et Parry, G. (2022). Perceptions of Transdisciplinary Engineering: Characterisations of the Transdisciplinary Research Approach. In B. R. Moser, B. R. Moser, P. Koomsap, & J. Stjepandic (Eds.), Transdisciplinarity and the Future of Engineering, *Proceedings of the 29th International Society of Transdisciplinary Engineering (ISTE) Global Conference*, Vol. 28, pp. 707-716, [En ligne] https://doi.org/10.3233/ATDE220704, Page consultée le 18 février 2023.

Gouvernment du Canada (2016). *Guide de gestion intégrée du risque : Approche recommandée pour la préparation d'un profil de risque organisationnel*, [En ligne] https://www.canada.ca/fr/secretariat-conseil-tresor/organisation/gestion-risque/guide-gestion-integree-risque.html, Page consultée le 10 janvier 2022.

Gouvernement du Québec (1999). *Pour affronter l’imprévisible : les enseignements du verglas de 98, Rapport de la Commission scientifique et technique chargée d’analyser les événements relatifs à la tempête de verglas survenue du 5 au 9 janvier 1998*, [En ligne] https://diffusion.mern.gouv.qc.ca, Page consultée le 19 janvier 2023.

Gouvernement du Québec (2008a). *Approches et principes en sécurité civile*, Ministère de la sécurité publique du Québec, [En ligne] https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/securite-publique/publications-adm/publications-secteurs/securite-civile/activites-formations/sc_formation_approche_principes.pdf, Page consultée le 1 mars 2025.

Gouvernement du Québec (2008b). *Concepts de base en sécurité civile*, Ministère de la sécurité publique du Québec, [En ligne] https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/securite-publique/publications-adm/publications-secteurs/securite-civile/activites-formations/sc_formation_concepts_base.pdf, Page consultée le 1 mars 2025.

Gouvernement du Québec (2022). *Modèle de politique en gestion intégrée des risques à l'intention des ministères et organismes assujettis à la loi sur l'administration publique*, [En ligne] https://www.tresor.gouv.qc.ca/fileadmin/PDF/cadre_gestion/Modele_politique-GIR.pdf, Page consultée le 19 janvier 2023.

Government of Canada (2016). *Guide to integrated risk management: A recommended approach for developing a corporate risk profile*, [En ligne] https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/guide-integrated-risk-management.html, Page consultée le 10 janvier 2022.

Government of Canada (2020). Team Charter Guidelines (TRN2-J04), [En ligne] https://www.csps-efpc.gc.ca/tools/jobaids/virtual-team-charter-eng.aspx, Page consultée le 15 septembre 2023.

Greco, T. F. (1995). *Unity of effort in peace operations*, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, [En ligne] https://apps.dtic.mil/sti/pdfs/ADA309917.pdf, Page consultée le 12 septembre 2024.

Habib, M., Lavergne, L. & Caparos, S. (2018). Chapitre 4. Perception. Dans : M. Habib, L. Lavergne & S. Caparos (Dir), Psychologie cognitive : Cours, méthodologie, exercices corrigés (pp. 96–127). Paris: Armand Colin. [En ligne] https://doi.org/10.3917/arco.habib.2018.01.0096, Page consultée le 4 janvier 2025.

Hamel, G. (2011). "First, lets fire all the managers", *Harvard Business Review*, December 2011, [En ligne] https://hbr.org/2011/12/first-lets-fire-all-the-managers, Page consultée le 15 août 2023.

Hergon, E., Moutel, G., Bellier, L., Hervé, C., and Rouger, P. (2004). "Les facteurs de perception et d'acceptabilité du risque : un apport pour la connaissance des représentations du risque transfusionnel", *Transfusion clinique et biologique*, Vol. 11 No. 3, pp. 130–137.

Heydari, M., Osanloo, M., et Başçetin, A. (2023). “Developing a new social impact assessment model for deep open-pit mines”, *Resources Policy*, Vol. 82, [En ligne] https://doi.org/10.1016/j.resourpol.2023.103485, Page consultée le 14 décembre 2023.

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*, 5th ed., New York: Kogan Page Publishers, ISBN: 978-0749483075, 480 pages.

Houmb, S. H. (2007). *Decision Support for Choice of Security Solution: The Aspect-Oriented Risk Driven Development (AORDD) Framework*, Thesis for the degree philosophiae doctor, Norwegian University of Science and Technology, Faculty of Information Technology, Trondheim, November 2007.

Huygens, C. (1714). The Value of All Chances in Games of Fortune, London: S. Keimer for T. Woodward, English translation 1714, [En ligne] https://math.dartmouth.edu/~doyle/docs/huygens/huygens.pdf, Page consultée le 23 septembre 2022.

Hwang, G. H. et Yoon, W. C. (2020). “A new approach to requirement development for a common operational picture to support distributed situation awareness”, *Safety Science*, Vol. 125, 2020, 104569, ISSN 0925-7535, [En ligne] https://doi.org/10.1016/j.ssci.2019.104569, Page consultée le 19 avril 2024.

IAEA (2015). *The Fukushima Daiichi Accident, Report by the Director General, International Atomic Energy Agency*, Vienna, [En ligne] https://www-pub.iaea.org/mtcd/publications/pdf/pub1710-reportbythedg-web.pdf, Page consultée le 19 janvier 2023.

IAIS (2013). Insurance core principles, standards, guidance and assessment methodology, October 2011, ICP 9 amended October 2012, ICP 22, amended October 2013.

IFMA (2024). What is facility management, International Facility Management Association, [En ligne] https://www.ifma.org/about/what-is-fm/, Page consultée le 17 mars 2024.

IGOPP (2022). *Pour une gouvernance créatrice de valeur*, [En ligne] https://igopp.org/ligopp/creation-de-valeurs/, Page consultée le 5 février 2023.

IIA (2020). *The IIA's three lines model: An update of the Three Lines of Defence*, The Institute of Internal Auditors, [En ligne] https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf, Page consultée le 11 avril 2023.

IIA (2022). *Maturity Model for Governance, Institute of Internal Auditors*, [En ligne] https://iia.no/wp-content/uploads/2023/06/Maturity-Model-for-Governance_1.edition-2022_final.pdf, Page consultée le 4 janvier 2024.

Innovation, Sciences et Développement économique Canada (2023). Principales statistiques relatives aux petites entreprises, Direction générale de la petite entreprise, [En ligne] https://ised-isde.canada.ca/site/sme-research-statistics/sites/default/files/documents/2023-ksbs-fr.pdf, Page consultée le 26 août 2025.

IRGC (2005). *Risk governance. Towards an integrative approach*, Lausanne: International Risk Governance Council (IRGC) [En ligne] https://irgc.org/wp-content/uploads/2018/09/IRGC_WP_No_1_Risk_Governance__reprinted_version_3.pdf, Page consultée le 20 novembre 2023.

IRGC (2017). *Introduction to the IRGC risk governance framework*, Lausanne: International Risk Governance Council (IRGC), [En ligne] https://infoscience.epfl.ch/record/233739, Page consultée le 20 novembre 2023.

IRGC (2018). *Guidelines for the Governance of Systemic Risks*, Lausanne: International Risk Governance Council (IRGC) from [En ligne] https://doi.org/10.5075/epfl-irgc-257279, Page consultée le 20 novembre 2023.

IRGC (2020). *Involving Stakeholders in the Risk Governance Process*, Lausanne: International Risk Governance Council (IRGC), [En ligne] https://doi.org/10.5075/epfl-irgc-282243, Page consultée le 22 novembre 2023.

ISACA (2012). *COBIT5: A business framework for the governance and management of enterprise IT*, Illinois: ISACA, ISBN: 978-1604202373, 94 pages.

ISACA (2018a). *COBIT2019 framework: Introduction and methodology*, Illinois: ISACA, ISBN: 978-1604207637, 64 pages.

ISACA (2018b). *COBIT2019 governance and management objectives,* Illinois: ISACA, ISBN: 978-1604207644, 302 pages.

ISO (2002). *ISO 31000:2002: Risk Management – Guidelines,* International Organization for Standardization, Geneva.

ISO (2009). *ISO 31000:2009: Risk Management – Guidelines,* International Organization for Standardization, Geneva.

ISO (2018). *ISO 31000:2018: Risk Management – Guidelines,* International Organization for Standardization, Geneva.

ISO (2019a). ISO 22301:2019: Security and Resilience – Business Continuity Management Systems Requirements, International Organization for Standardization, Geneva.

ISO (2019b). ISO 31010:2019: Risk Management – Risk Assessment Techniques, 2nd Edition, International Organization for Standardization, Geneva.

ISO (2023a). "Consumers and standards: partnership for a better world", [En ligne] https://www.iso.org/sites/ConsumersStandards/index.html, Page consultée le 17 juin 2023.

ISO (2023b). ISO 37004:2023: Governance of organizations — Governance maturity model — Guidance (Edition 1), International Organization for Standardization, Geneva.

Jacob, R. et Michel, G. (2020). *La gestion en mode matriciel et transversal et la gestion agile et organique dans les organisations : Apprentissages pour la fonction publique Québécoise*, Pôle Santé, HAC Montréal, Juillet 2020, [En ligne] http://dx.doi.org/10.13140/RG.2.2.12840.65280, Page consultée le 27 novembre 2023.

Jean-Jules, J. et Vicente, R. (2020). "Rethinking the implementation of enterprise risk management (ERM) as a socio-technical challenge", *Journal of Risk Research*, Vol.24, No. 2, pp.247–266.

Jodelet, D. (2001). Le phénomène Nimby. Dans : Michel Boyer éd., L'Environnement, question sociale : Dix ans de recherche pour le ministère de l'Environnement (pp. 91–97). Paris: Odile Jacob, [En ligne] https://doi.org/10.3917/oj.roche.2001.01.0091, Page consultée le 17 février 2025.

Jousse, G. (2009). *Traité de riscologie : La science du risque*, Les éditions Imestra, ISBN 978-2-9509-8887-4, 598 pages.

Ju, Y., and You, M. (2022). “It’s politics, isn’t it? Investigating direct and indirect influences of political orientation on risk perception of COVID-19”, *Risk Analysis*, Vol. 42 No. 1, pp. 56–68, https://doi.org/10.1111/risa.13801.

Kaplan, R.S. et Norton, D.P. (1996). *The Balanced Scorecard – Translating Strategy into Action*. Harvard Business School Press, Boston.

Kélada, J. (1994). *La méthode AMDEC*, Centre d’études en qualité totale, École des hautes études commerciales, [En ligne] http://neumann.hec.ca/sites/cours/6-510-96/AMDEC.pdf, Page consultée le 13 mars 2024.

Keynes, J. M. (1936). *The General Theory of Employment, Interest and Money*, 1960 Edition, London: Palgrave MacMillan, ISBN: 978-0333009420, 463 pages.

Kingsley, R. (2017a). “The fundamental principle of «Unity of effort» in multinational operations”, *Military caveats*, [En ligne] http://militarycaveats.com/7-the-fundamental-principle-of-unity-of-effort-in-multinational-operations/, Page consultée le 4 mai 2024.

Kingsley, R. (2017b). “The «Unity of effort model» & multinational commanders: Vital for success in multinational operations”, *Military caveats*, [En ligne] http://militarycaveats.com/8-the-unity-of-effort-model-vital-for-success-in-multinational-operations/, Page consultée le 4 mai 2024.

Kmiec, R. et Roland-Lévy, C. (2014). “Risque et construction sociale : une approche interculturelle”, *Les cahiers internationaux de psychologie sociale*, Vol. 101 No. 1, pp. 69–99.

Knight, F. H. (1921). *Risk, Uncertainty and Profit*, Boston and New York: Houghton Mifflin Company, 388 pages, [En ligne] https://fraser.stlouisfed.org/files/docs/publications/books/risk/riskuncertaintyprofit.pdf, Page consultée le 19 novembre 2023.

Kodama, M. (2005a). “Knowledge Creation through Networked Strategic Communities: Case Studies on New Product Development in Japanese Companies”, *Long Range Planning*, Vol. 38, pp. 27–49.

Kodama, M. (2005b). “New knowledge creation through leadership-based strategic community: A case of new product development in IT and multimedia business fields”, *Technovation*, Vol. 25 No. 8, pp. 895–908.

Kodama, M. (2007). “Innovation and knowledge creation through leadership-based strategic community: Case study on high-tech company in Japan”, *Technovation*, Mars 2007, Vol. 27, No. 3, pp 115–132.

Koh, S.C.L., Gunasekaran, A., et Rajkumar, D. (2008). “ERPII: The involvement, benefits and impediments of collaborative information sharing”, *International Journal of Production Economics*, Vol. 113, Issue 1, pp. 245–268.

ICSI (2021). “Perception des risques et de l’alerte, comportements des populations : ce que la psychologie nous apprend”, *Risques industriels et territoire*, Institut pour une culture de sécurité industrielle, 10 Juin 2021, [En ligne] https://www.icsi-eu.org/perception-risques-alerte-comportements-populations-psychologie, Page consultée le 21 février 2025.

Komljenovic, D., Gaha, M., Abdul-Nour, G., Langheit, C. et Bourgeois, M. (2016). “Risks of extreme and rare events in Asset Management”, *Safety Science*, Vol. 88, pp 129–145.

Kouabénan, D. R., Cadet, B., Hermand, D. & Muñoz Sastre, M. T. (2007). Chapitre 6. Des facteurs structurants aux biais ou illusions dans la perception des risques. Dans : Dongo Rémi Kouabénan éd., Psychologie du risque (pp. 77–89). Louvain-la-Neuve: De Boeck Supérieur, [En ligne] https://doi.org/10.3917/dbu.kouab.2007.01.0077, Page consultée le 16 février 2025.

Kouabénan, D. R., Cadet B., Hermand, D., Muñoz Sastre, M.T. (2006). Psychologie du risque : Identifier, évaluer, prévenir, Bruxelles: De Boeck, 346 pages.

Kuraoka, S., Paudyal, Y. R. et Razak, K. A. (2020). “Transdisciplinary approach for building societal resilience to disasters – Interpreting the processes of creating new knowledge in the context of knowledge management”, *Journal of Disaster Research*, Vol. 15 No. 7, pp. 868–877.

Lacroix, I. et St-Arnaud, P.-O. (2012). “La gouvernance : tenter une définition”, *Cahiers de recherche en politique appliquée*, Vol. 4 No. 3, pp. 19–37.

Lagadec, P. (2000). Ruptures créatrices, Édition d’Organisation, 640 pages.

Lee, J. et Wong, E. (2021). “Suez Canal blockage: An analysis of legal impact, risks and liabilities to the global supply chain”, *MATEC Web of Conferences*, 339, [En ligne] https://doi.org/10.1051/matecconf/202133901019, Page consultée le 19 novembre 2023.

Luokkala, P., Nikander, J., Korpi J., Virrantaus, K. et Torkki, P. (2016). “Developing a concept of a context-aware common operational picture”, *Safety Science*, Vol. 93, pp 277–295.

Martelletti, C. P., Santirocchi, A., Spataro, P., Rossi-Arnaud, C., Löfstedt, R. E., & Cestari, V. (2022). “Predictors of COVID-19 risk perception, worry and anxiety in Italy at the end of the 2020 national lockdown”, *Journal of Risk Research*, 25(11–12), pp. 1306–1320, [En ligne] https://doi.org/10.1080/13669877.2022.2038245, Page consultée le 3 mars 2025.

Martinez, F. (2010). “L'individu face au risque : l'apport de Kahneman et Tversky”, Idées économiques et sociales, No. 161, pp. 15–23, [En ligne] https://doi.org/10.3917/idee.161.0015, Page consultée le 19 février 2025.

Micouleau, D. et Robert, B. (2021). “Case study: Development of an integrative approach to assess municipalities’ resilience potential”. *International Journal of Business Continuity and Risk Management*, Vol. 11 No. 1, pp. 66–78.

Micouleau, D., Robert, B. et Hémond, Y. (2020). “Conceptual framework for organizational adaptability in a context of disruption management”, *Business and Management Research Journal*, Vol. 10 No. 8, pp. 150–156.

Mills, B. (2020). “An updated assessment of lightning-related fatality and injury risk in Canada: 2002–2017”, *Natural Hazards*, Vol. 102, pp.997–1009, https://doi.org/10.1007/s11069-020-03942-9.

Ministère de l’Éducation du Québec (2006). Chapitre 3 : Les compétences transversales, Dans : Programme de formation de l’école québécoise, enseignements secondaire et premier cycle, Ministère de l’Éducation du Québec, [En ligne] https://www.education.gouv.qc.ca/fileadmin/site_web/documents/PFEQ/chapitre003v2.pdf, Page consultée le 4 décembre 2023.

Mongeau, P. et Saint-Charles, J. (2024). Groupe et animation : théories et pratiques, Université du Québec à Montréal, 151 pages, [En ligne] https://groupeetanimation.uqam.ca/pdf/, Page consultée le 2 septembre 2025.

Morabito, L., et Lagacé-Banville, J. (2013). “Préparation aux situations d’urgence : Simulation d’une pénurie d’eau à Montréal”, *InterAction*, Vol. 4, No. 1, p. 8.

Morabito, L., et Robert, B. (2015). *Formalizing a framework for the exchange and sharing of information in the telecommunications sector*, Defence Research and Development Canada, December 2015, 45p.

Morabito, L. et Robert, B. (2023a). “Success factors and lessons learned during the implementation of a cooperative space for critical infrastructures”, *Int. J. Critical Infrastructures*, Vol. 19 No. 6, pp.527–543.

Morabito, L. et Robert, B. (2023b). “Challenges related to emerging risk management”, *International Journal of Risk Assessment and Management*, Vol. 26, No. 2, pp.175–195.

Morabito, L. et Robert, B. (2025). “A governance framework for achieving transversal and strategic integration of risk management in large organizations”, *Int. J. Decision Sciences, Risk and Management*, Vol. x, No. x, pp.xx–xx.

Nasiri, H., Yusof, M. J. M., Ali, T. A. M., et Hussein, M. K. B. (2019). “District flood vulnerability index: urban decision-making tool”, *International Journal of Environmental Science and Technology*, Vol. 16 No. 5, pp. 2249–2258.

Niget, D., and Petitclerc, M. (2012). “Pour une histoire du risque : Québec, France, Belgique”, 1st ed., Presses de l’Université du Québec, 368 pages.

NIST (2008). *Volume 1: Guide for mapping types of information and information systems to security categories*, Special publication 800-60, Vol. 1, Revision 1, U.S. Department of Commerce, August 2008, [En ligne] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v1r1.pdf, Page consultée le 22 octobre 2023.

NIST (2018a). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute of Standards and Technology, U.S. Department of Commerce, April 2018, [En ligne] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, Page consultée le 22 octobre 2023.

NIST (2018b). *Risk Management Framework for Information Systems and Organizations : A System Life Cycle Approach for Security and Privacy Framework for Improving Critical*

Infrastructure Cybersecurity, NIST Special Publication 800-37, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce, December 2018, [En ligne] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, Page consultée le 22 octobre 2023.

NIST (2024). The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, [En ligne] https://doi.org/10.6028/NIST.CSWP.29, Page consultee le 21 mars 2024.

NRC et US DOE (2004). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, Canada–U.S. Power System Outage Task Force, [En ligne] https://emp.lbl.gov/publications/final-report-august-14-2003-blackout, Page consultée le 23 mai 2023.

NRC et US DOE (2006). *U.S.-Canada Power System Outage Task Force – Final report on the implementation of the task force recommendations*, Natural Resources Canada and U.S. Department of Energy, [En ligne] https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/BlackoutFinalImplementationReport%282%29.pdf, Page consultée le 16 juillet 2023.

OECD (2003). *Emerging Systemic Risks in the 21st Century: An Agenda for Action*, Organization for Economic Co-operation and Development, [En ligne] https://www.oecd.org/futures/globalprospects/37944611.pdf, Page consultée le 4 janvier 2023.

Oliveira, K., Méxas, M., Meiriño, M. et Drumond, G. (2019). “Critical success factors associated with the implementation of enterprise risk management”, *Journal of Risk Research*, Vol. 22 No. 8, pp. 1004–1019.

Palmer, M.A. (2023). “Explainer: What Is a Shared Mental Model? Why Are Mental Models Useful for Interdisciplinary Research?”, National Socio-Environmental Synthesis Center (SESYNC), [En ligne] https://www.sesync.org/sites/default/files/2023-06/Explainer%20%E2%80%93%20What%20Is%20a%20Shared%20Mental%20Model.pdf, Page consultée le 16 mai, 2025.

Peerenboom, J.P., Fisher, R.E., Rinaldi, S.M., et Kelly, T.K. (2002). “Studying the chain reaction”, *Electric Perspectives*, January–February, pp. 22–31.

Perfors, A., et Van Dam, N. T. (2018). “Human decision making in black swan situations”, In Proceedings of the 40th Annual Meeting of the Cognitive Science Society, CogSci 2018, pp. 870-875, The Cognitive Science Society.

Pescaroli, G., et Kelman, I. (2017). “How critical infrastructure orients international relief in cascading disasters”, *Journal Contingencies Crisis Management*, Vol. 25, Issue 2, pp. 56–67.

Petrenj, B., Lettieri, E. et Trucco, P. (2012). “Towards enhanced collaboration and information sharing for critical infrastructure resilience: current barriers and emerging capabilities”, *International Journal of Critical Infrastructures*, Vol. 8, Nos. 2/3, pp.107–120.

Pilemalm, S. and Yousefi Mojir, K. (2020). “ICT enabled cross-sector coopération in emergency response: emerging forms of public-sector network governance”, *International Journal of Emergency Management*, Vol. 16, No. 3, pp.249–280.

PMI (2017). A guide to the Project Management Body of Knowledge (PMBOK guide), 6th ed., Newton Square, PA, Project Management Institute.

PMI (2021). A guide to the Project Management Body of Knowledge (PMBOK guide), 7th ed., Newton Square, PA, Project Management Institute.

Purdy, G. (2010). “ISO 31000:2009 – Setting a new standard for risk management”, *Risk Analysis*, Vol. 30 No. 6, pp. 881–886.

Rao, R. (2007). “Connecting organization strategy to projects - the missing link”, Paper presented at PMI® Global Congress 2007 - Asia Pacific, Hong Kong, People's Republic of China. Newtown Square, PA: Project Management Institute.

Ray-Bennett, N. S., Masys, A., Shiroshita, H. et Jackson, P. (2014). “Hyper-risks in a hyper-connected world: A call for critical reflective response to develop organizational resilience”, *Global Assessment Report on Disaster Risk Reduction 2015*, United Nations Office for Disaster Risk Reduction, January 2014, [En ligne] https://www.preventionweb.net/english/hyogo/gar/2015/en/bgdocs/Ray-Bennett%20et%20al.,%202014.pdf, Page consultée le 20 octobre 2023.

RCCTT (2023). “Quelles sont les méthodes de la recherche scientifique ?”, Réseaux des Centres Collégiaux de transfert de technologies, 16 Juillet 2023, [En ligne] https://reseaucctt.ca/actualites/methode-recherche-scientifique, Page consultée le 15 octobre 2024.

Reason, J., Hollnagel, E. et Paries, J. (2006). “Revisting the «Swiss cheese» model of accidents”, Eurocontrol, European organisation for the safety of air navigation, Note 13/06, [En ligne] https://www.eurocontrol.int/sites/default/files/library/017_Swiss_Cheese_Model.pdf, Page consultée le 17 juin 2023.

Renaud, L. (2020). “Modélisation du processus de la recherche participative”, *Communiquer*, No 30, 2020, [En ligne] https://www.erudit.org/fr/revues/communiquer/2020-n30-communiquer05695/1073806ar/, Page consultée le 4 octobre 2024.

Rinaldi, S.M., Peerenboom, J.P., et Kelly, T.K. (2001). “Identifying, understanding, and analyzing critical infrastructures interdependencies”, *IEEE Control Systems Magazine*, Vol. 21, Issue 6, pp. 11–25.

Robert, B., Arnoux, J., et Morabito, L. (2015). “Understanding the impediments to inter-organizational information sharing: Application to the telecommunications sector”, *Infrastructure Resilience Research Group Journal*, Vol. 1, Issue 4, pp. 3–11.

Robert, B., de Calan, R., et Morabito, L. (2008). “Modelling interdependencies among critical infrastructures”, *International Journal of Critical Infrastructures*, Vol. 4, Issue 4, pp. 392–408.

Robert, B., Delvosalle, C., Nourry, J., et Morabito, L. (2014). “Identifying critical infrastructures’ vulnerability to the transportation of dangerous goods”, *The CIP Report*, Vol. 13, Issue 2, pp. 5–8.

Robert, B., Hémond, Y., et Salas Useche, L. F. (2019). “Resilience of interdependent critical infrastructures: A case study in Québec (Canada)”, *2019 International Conference on High Performance Computing & Simulation (HPCS)*, pp. 589–594, [En ligne] https://doi: 10.1109/HPCS48598.2019.9188192, Page consultée le 19 octobre 2023.

Robert, B., Hémond, Y., et Yan G. (2013). “L’évaluation de la résilience organisationnelle”, *La gestion des risques majeurs : La résilience organisationnelle, apprendre à être surpris*, Éditions Yvon Blais, Chapitre 3, pp.151–188.

Robert, B. et Morabito, L. (2008). “The operational tools for managing physical interdependencies among critical infrastructures”, *International Journal of Critical Infrastructures*, Vol. 4, Issue 4, pp. 353–367.

Robert, B. et Morabito, L. (2009). “Dependency on electricity and telecommunications”, *Securing electricity supply in the cyber age: Exploring the risks of information and communication technology in tomorrow’s electricity infrastructure*, Chapter 3, Dordrecht: Springer Netherlands.

Robert, B. et Morabito, L. (2010a). “An approach to identifying geographic interdependencies among critical infrastructures”, *International Journal of Critical Infrastructures*, Vol. 6, Issue 1, pp. 17–30.

Robert B. et Morabito L. (2010b). “Modeling of Critical Infrastructure Interdependencies”. URSCorp, Washington, DC, March 16, 2010.

Robert, B. et Morabito, L. (2011). *Reducing vulnerability of critical infrastructures*, Montreal: Presses internationales Polytechnique.

Robert, B. et Morabito, L. (2013). “Risque majeurs et interdépendances entre les systèmes essentiels”, *La gestion des risques majeurs : La résilience organisationnelle, apprendre à être surpris*, Éditions Yvon Blais, Chapitre 4, pp.189–223.

Robert, B., Morabito, L., et Cloutier, I. (2012). “Modeling and coordinating interdependent critical infrastructures in Montréal”, *The CIP Report*, Vol. 10, Issue 11, pp. 3–6.

Robert, B., Morabito, L., et Debernard, C. (2013). “Simulation and anticipation of domino effects among critical infrastructures”, *International Journal of Critical Infrastructures*, Vol. 9, Issue 4, pp. 275–303.

Robert, B., Morabito, L. et Quenneville, O. (2007). “The preventive approach to risks related to interdependent infrastructures”, Int. J. Emergency Management, Vol. 4 No. 2, pp. 166–182.

Roy, M., Audet, M., Gosselin, A., Lortie, P.B., et Fortier, L. (2011). “La communauté stratégique: une approche pour développer la collaboration interorganisationnelle”, [En ligne] https://www.usherbrooke.ca/ceot/fileadmin/sites/ceot/documents/Publications/Rapports_de_recherche/rapport_fcrss.pdf, Page consultée le 1 mai 2021.

Roy, M., Audet, M., Gosselin, A., Fortier, L., et Lortie, P. B. (2012). “Guide de mise en place d’une communauté stratégique pour améliorer la collaboration et l’organisation du travail interétablissements”, Université de Sherbrooke, [En ligne] https://www.inspq.qc.ca/sites/default/files/documents/itss/guide_communaute_strategique_2012.pdf, Page consultée le 1 mai 2021.

Roy, M., Audet, M., Gosselin, A., Lortie, P. B. et Fortier, L. (2013). “La communauté stratégique: une approche pour développer la collaboration interorganisationnelle”, [En ligne] http://www.fcass-cfhi.ca/Libraries/Reports/Strategic-Community-InterOrg-Collab-Roy-F.sflb.ashx, Page consultée le 1 mai 2021.

Roy, M. et Prévost, P. (2013). “La recherché-action : origines, caractéristiques et implications de son utilisation dans les sciences de la gestion”, *Recherches qualitatives*, Vol. 32, No 2, pp. 129–151, https://doi.org/10.7202/1084625ar.

Runde, J. (1990). “Keynesian uncertainty and the weight of arguments”, *Economics and Philosophy*, Vol. 6 No. 2, pp. 275–292.

Salim, A., Pepperill, A, Mitchell, C., Candy, C., Long, J., Acker, M., Karlsson-Brown, P., Beaton, R., Nolan, S., Walsh, S., Brown, S., Griffiths, S. et Lumsden, T. (2021). “*An Introduction to Emerging Risks and How to Identify Them: IRM Charities Special Interest Group Report*”, Institute of Risk Management, [En ligne] https://www.theirm.org/media/9230/charities-sig-an-introduction-to-emerging-risks-and-how-to-identify-them.pdf, Page consultée le 5 février 2023.

Samuel, K.E., et Spalanzani, A. (2009). “Developing collaborative competencies within supply chains”, *International Journal of Information Technology and Management*, Vol. 8, Issue 2, pp. 146–160.

Sarker, S., Engwall, M., Trucco, P. and Feldman, A. (2016). “Internal Visibility of External Supplier Risks and the Dynamics of Risk Management Silos”, *IEEE transactions on engineering management*, Vol. 63, No. 4, pp 451–461.

Schnewlin, C. (2024). “Turning failure into opportunity: Resilience by Design”, [En ligne] https://www.ey.com/en_ch/insights/technology/turning-failure-into-opportunity-resilience-by-design, Page consultée le 6 juin 2025.

Schraagen, J.M., Huis in ‘t Veld, M. and de Koning, L. (2010). “Information Sharing During Crisis Management in Hierarchical vs. Network Teams”, *Journal of Contingencies and Crisis Management*, Vol. 18, No. 2, pp 117–127.

Seppänen, H., Mäkelä, J., Luokkala, P. and Virrantaus, K. (2013). “Developing shared situational awareness for emergency management”, *Safety Science*, 55 (2013), pp. 1–9.

Simard, P. (2007). “Développer une théorie de l’action pour une démarche communautaire. Comment définir les visées d’une démarche et les principes d’action”. In GAGNON, C. (Éd) et E., ARTH (en collab. avec). Guide québécois pour des Agendas 21e siècle locaux : applications territoriales de développement durable viable, [En ligne] http://www.a21l.qc.ca/9546_fr.html, Page consultée le 4 janvier 2023.

Shah. P., Yang, J.Z., et Kahlor, L. (2023). “Psychological distance, risk perception, and affect: Texas residents’ support for carbon capture and storage”, *Journal of Risk Research*, Vol. 26 No. 2, pp. 184–198.

Sjöberg, L. (2000). “Factors in risk perception”, *Risk Analysis*, Vol. 20 No. 1, pp. 1–12. Standards Australia. (2004) *AS/NZS 4360:2004: Risk Management*, Standards Australia, Sydney.

Skøt, L., Nielsen, J. B., et Leppin, A. (2021). “Risk perception and support for security measures: interactive effects of media exposure to terrorism and prior life stress?” *Journal of Risk Research*, Vol 24 No 2, pp. 228–246. https://doi.org/10.1080/13669877.2020.1750460

Standards Australia. (2004). AS/NZS 4360:2004: Risk Management, Standards Australia, Sydney.

Stevens, R., Votipka, D., Dykstra, J., Tomlinson, F., Quartararo, E., Ahern, C. and Mazurek, M. L. (2022). “HowReady is Your Ready? Assessing the Usability of Incident Response Playbook Frameworks”, CHI Conference on Human Factors in Computing Systems (CHI ’22), 29 avril

au 5 mai 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 18 pages. [En ligne] https://doi.org/10.1145/3491102.3517559, Page consultée le 17 juin 2024.

Stohs, M. (1980). ““Uncertainty” in Keynes’ general theory”, *History of Political Economy*, Vol. 12 No. 3, pp. 372–382.

Stripe (2024). Stratégies de gestion du changement que chaque entreprise devrait connaître, [En ligne] https://stripe.com/fr-ca/resources/more/change-management-strategies-every-business-should-know, Page consultée le 2 septembre 2025.

Su, F. (2021). “The chaos theory and its application”, *Journal of Physics: Conference Series*, Vol.. 2012 No. 1, [En ligne] https://iopscience.iop.org/article/10.1088/1742-6596/2012/1/012118/pdf, Page consultée le 17 novembre 2023.

Szántó, R. et Dudás, L. (2022). “COVID-19 skepticism and the perception of risk”, *Journal of Risk Research*, https://doi.org/10.1080/13669877.2022.2107051

Taleai, M. et Mansourian, A. (2008). “Using Delphi-AHP method to survey major factors causing urban plan implementation failure”, Journal of Applied Sciences, Vol. 8 No. 15, pp. 2746–2751.

Taleb, N. N. (2010). *The Black Swan: Second Edition: The Impact of the Highly Improbable: With a new section: “On Robustness and Fragility*”, New York: Random House Trade, ISBN: 978-0812973815, 480 pages.

Tašner, V. et Gaber, S. (2020). “Lev Vygotski, initiateur du constructivisme social et penseur insaisissable de l’éducation”, *Revue internationale d’éducation de Sèvres*, Vol. 79, pp. 109–116.

Tena-Chollet, F. (2012). “Élaboration d’un environnement semi-virtuel de formation à la gestion stratégique de crise, basé sur la simulation multi-agents”, Doctoral Thesis, École Nationale Supérieure des Mines de St-Etienne.

Tena-Chollet, F., Tixier, J., Dandrieux, A. et Slangen, P. (2017). “Training decision-makers: Existing strategies for natural and technological crisis management and specifications of an improved simulation-based tool”, *Safety Science*, Vol. 97, pp. 144–153.

TEPCO (2012). *Fukushima Nuclear Accident Analysis Report*, Tokyo Electric Power Company Inc., [En ligne] https://www.tepco.co.jp/en/press/corp-com/release/betu12_e/images/120620e0104.pdf, Page consultée le 29 janvier 2023.

Thacker, S., Pant, R. and Hall, J. W. (2017). "System-of-systems formulation and disruption analysis for multi-scale critical national infrastructures", *Reliability Engineering and System Safety*, Vol. 167, pp. 30–41.

Trucco, P. and Petrenj, B. (2017). "Resilience of Critical Infrastructures: benefits and challenges from emerging practices and programs at local level", *Resilience and Risk, Methods and Application in Environment, Cyber and Social Domains*, Chapter 10, Springer, pp. 225–286.

Tversky, A. and Kahneman, D. (1974). "Judgment under Uncertainty: Heuristics and Biases", *Science, New Series*, Vol. 185, No. 4157, pp. 1124–1131.

UCTE (2007). *System disturbance on 4 November 2006 – Final report*, Union for Co-ordination of Transmission of Electricity, [En ligne] http://ecolo.org/documents/documents_in_english/blackout-nov-06-UCTE-report.pdf, Page consultée le 13 mai 2021.

UNDRR (2015). *The 2015-2030 Sendai Framework for Disaster Risk Reduction*, Geneva: United Nations Office for Disaster Risk Reduction, [En ligne] https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030, Page consultée le 18 février 2023.

UNDRR (2019). *Global Assessment Report on Disaster Risk Reduction 2019*, Geneva: United Nations Office for Disaster Risk Reduction, [En ligne] https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2019, Page consultée le 19 janvier 2023.

US DOD (2009). *The Dictionary of Military Terms*, Joint Pub 1-02, New York, Skyhorse Publishing, 2009, p. 360.

US DHS (2014). Control Systems Cyber Security: Defense in Depth Strategies, CreateSpace Independent Publishing Platform, 30 pages.

Vézina, M., and Messier, C. (2009). "L'apprentissage interorganisationnel et la pérennisation de la collaboration partenariale : Le cas d'une banque solidaire", 2e colloque sur le Management

relationnel et Collaboration, Acte du 77e congrès de l'Association Canadienne-Française pour l'Avancement des Sciences (ACFAS), Ottawa: Université d'Ottawa, [En ligne] http://www.chaire-msf.uqam.ca/pages/pdf/vezina-messier.pdf, Page consultée le 8 mars 2021.

Vygotsky, L. S. (1978). *Mind in Society: The Development of Higher Psychological Processes*, Cambridge (MA): Harvard University Press, ISBN-0674576292, 176 pages.

Wachinger, G., Renn, O., Begg, C., & Kuhlicke, C. (2013). "The risk perception paradox-implications for governance and communication of natural hazards", *Risk Analysis*, Vol. 33 No. 6, pp. 1049–1065. https://doi.org/10.1111/j.1539-6924.2012.01942.x

Wang, Y., Shen, C., Bartsch, K., and Zuo, J. (2021a). "Exploring the trade-off between benefit and risk perception of NIMBY facility: A social cognitive theory model", *Environmental Impact Assessment Review*, Vol. 87, https://doi.org/10.1016/j.eiar.2021.106555

Wang, C., Geng, L., and Rodríguez-Casallas, J. D. (2021b). "How and when higher climate change risk perception promotes less climate change inaction", *Journal of Cleaner Production*, Vol. 321. https://doi.org/10.1016/j.eiar.2021.106555

Whitaker, L. (2016). "Enterprise Risk Management Framework as an Ecosystem", 2016 Enterprise Risk Management Symposium, April 6–8, 2016, Arlington, Virginia, [En ligne] https://www.soa.org/globalassets/assets/files/resources/essays-monographs/2016-erm-symposium/mono-2016-erm-whitaker.pdf, Page consultée le 16 mai 2025.

Wilder, M.K. (2012). "Achieving Unity of Effort", *InterAgency Journal*, Vol. 3 No. 1, pp. 40–46.

Zhao, P., Ali, M. Z. and Ahmad, Y. (2023). "Developing indicators for sustainable urban regeneration in historic urban areas: Delphi method and Analytic Hierarchy Process (AHP)", *Sustainable Cities and Society*, Vol. 99, 2023, https://doi.org/10.1016/j.scs.2023.104990.