POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Vers une compréhension partagée de l'environnement technologique : une approche collaborative en milieu organisationnel

MARIE-CLAUDE PAQUETTE

Département de mathématiques et de génie industriel

Mémoire présenté en vue de l'obtention du diplôme de *Maîtrise ès sciences appliquées*

Génie industriel

Août 2025

© Marie-Claude Paquette, 2025.

POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Ce mémoire intitulé :

Vers une compréhension partagée de l'environnement technologique : une approche collaborative en milieu organisationnel

présenté par **Marie-Claude PAQUETTE**

en vue de l'obtention du diplôme de *Maîtrise ès sciences appliquées*

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

Christophe DANJOU, président

Benoît ROBERT, membre et directeur de recherche

Yannick HÉMOND, membre

REMERCIEMENTS

Je tiens surtout à remercier mon directeur de recherche, Benoît Robert. Merci pour votre grande patience, votre flexibilité et votre accompagnement tout au long de cette démarche. Vous m'avez amenée à repousser les limites de mes réflexions qui depuis plusieurs années, s'étaient bien souvent retrouvées confinées à mon univers professionnel restreint. Merci d'avoir eu l'énergie nécessaire pour m'encadrer dans un environnement académique entièrement hors de ma zone de confort. Et finalement, merci d'avoir soupoudré nos échanges et nos désaccords de votre affable sens de la répartie.

Je souhaite remercier les membres du jury pour le temps consacré à l'évaluation de ce mémoire, dont sa lecture et sa soutenance.

Enfin, merci à tous ceux qui, à un moment ou un autre, ont été consultés et ont pris le temps de m'aider et m'éclairer dans ce projet.

RÉSUMÉ

Dans un contexte de croissance de l'adoption des technologies numériques, les opérations des organisations peuvent se retrouver vulnérables aux perturbations. Face à cette réalité, l'élaboration de stratégies de continuité des activités est essentielle, bien que souvent entravée par un manque de compréhension commune de l'environnement technologique entre les gestionnaires, l'équipe de continuité et l'équipe TI. Cette absence de synergie mène à une collaboration complexe et à un manque d'alignement dans les activités de préparation aux perturbations, se traduisant par des stratégies de continuité des activités potentiellement incomplètes ou divergentes.

S'inscrivant dans la continuité des recherches du Centre Risque & Performance, ce projet propose une démarche collaborative pour pallier ce problème en créant et en validant une Image Situationnelle Commune (ISC). Pour élaborer cette ISC, les logiciels d'application, et plus précisément les logiciels de bureautique de type SaaS, ont été sélectionnés pour leur position stratégique en tant que points de référence communs pour tous les intervenants de l'organisation. Ce choix a été reconfirmé lors d'un exercice de validation qui a prouvé que ce type de logiciels, bien qu'omniprésent dans l'organisation, est souvent sous-estimé dans les stratégies de continuité des activités. L'ISC proposée dans cette étude repose donc sur une vision holistique des logiciels de bureautique de type SaaS, créée à partir d'informations provenant de trois angles d'analyse : le type d'utilisation, les modalités d'utilisation et la portée d'utilisation. L'ISC est alors créée par la consolidation et la comparaison d'informations recueillies auprès des gestionnaires et de l'équipe TI, pour être ensuite validée lors d'un atelier. Ce dernier vise à stimuler les échanges, une prise de conscience collective et, ultimement, une compréhension commune de l'environnement technologique et de son utilisation qui est à la base d'une collaboration durable.

L'efficacité de la démarche proposée a été confirmée lors d'un exercice de validation en milieu municipal. L'atelier a prouvé sa capacité à générer des discussions essentielles, approfondissant la connaissance commune de l'environnement technologique et révélant des lacunes, notamment en ce qui concerne la formalisation des stratégies de continuité des activités. Les activités nécessaires à la création de l'ISC ont ultimement renforcé la collaboration entre l'équipe de continuité et l'équipe TI. Les résultats obtenus offrent donc des bases solides pour des itérations futures et pour l'élargissement et l'adaptation de l'approche à d'autres contextes et organisations.

ABSTRACT

In a context of growing adoption of digital technologies, the operations of organizations can find themselves vulnerable to disruptions. Faced with this reality, the development of business continuity strategies is essential, but it is often hindered by a lack of common understanding of the technological environment among managers, the business continuity team, and the IT team. This absence of synergy leads to complex collaboration and a lack of alignment in disruption preparedness, resulting in potentially incomplete or divergent business continuity strategies.

Following the research from the Centre risque & performance, this project proposes a collaborative approach to address this problem by creating and validating a Common Situational Image (CSI). To develop this CSI, application software, and more specifically office software, were selected for their strategic position as common reference points for all organizational stakeholders. This choice was reconfirmed during a validation exercise which proved that this type of software, although ubiquitous in organizations, is often underestimated in business continuity strategies. The CSI proposed in this study therefore relies on a holistic vision of office software, created from information derived from three angles of analysis: type of use, usage modalities, and scope of use. The CSI is then created by consolidating and comparing information gathered from managers and the IT team, to be subsequently validated during a workshop. The latter aims to stimulate discussions, foster collective awareness, and, ultimately, achieve a common understanding of the technological environment and its use, which is at the core of a durable collaboration.

The effectiveness of the proposed approach was confirmed during a validation exercise in a municipal context. The workshop proved its ability to generate essential discussions, deepening the common understanding of the technological environment and revealing gaps, particularly concerning the formalization of business continuity strategies. The activities necessary for the creation of the CSI ultimately strengthened collaboration between the continuity team and the IT team. The results obtained thus offer a solid basis for future iterations and for the expansion and adaptation of the approach to other contexts and organizations.

TABLE DES MATIÈRES

REMERCIEMENTS III

RÉSUMÉ IV

ABSTRACT V

LISTE DES FIGURES IX

LISTE DES SIGLES ET ABRÉVIATIONS X

LISTE DES ANNEXES XI

CHAPITRE 1 INTRODUCTION 1

CHAPITRE 2 ÉTAT DES CONNAISSANCES 3

2.1 Comprendre les technologies numériques en contexte d'une organisation 3

2.1.1 Logiciels d'application 3

2.1.2 Logiciels de système 4

2.1.3 Équipements informatique 4

2.1.4 Prise en charge des technologies numériques 4

2.2 Perturbations des logiciels d'application 6

2.2.1 Origine et ampleur 7

2.2.2 Manifestations des perturbations 9

2.3 Continuité des activités et reprise informatique 10

2.3.1 Plan de continuité des activités 11

2.3.2 Plan de reprise informatique 13

2.3.3 Points d'intersection 14

2.3.4 Prise en charge des perturbations 15

2.4 Notions de vulnérabilité 15

CHAPITRE 3 CONSTATS 18

CHAPITRE 4 CADRE ET DÉMARCHE DE RECHERCHE 21

4.1 Cadre de la recherche 21

4.2 Objectifs de la recherche 23

4.3 Méthodologie 24

CHAPITRE 5 ÉLABORATION DE L'ISC 26

5.1 Bases de l'ISC dans un contexte de technologies numériques 26

5.2 Dimensions de l'ISC 29

5.2.1 Type d'utilisation 30

5.2.1.1 Outils de communication 30

5.2.1.2 Outils d'organisation 31

5.2.1.3 Outils de collaboration 31

5.2.2 Modalités d'utilisation 32

5.2.3 Portée d'utilisation 33

5.2.4 Validation des dimensions 33

5.3 Proposition d'une démarche pour initier une approche collaborative 35

5.3.1 Étape 1 : former l'équipe et comprendre les besoins 35

5.3.2 Étape 2 : caractérisation de l'ISC 36

5.3.3 Étape 3 : collecte d'informations 38

5.3.4 Étape 4 : création de l'ISC 40

5.3.5 Étape 5 : validation de l'ISC 41

5.3.6 Étape 6 : application des constats issus de la validation de l'ISC 42

CHAPITRE 6 EXERCICE DE VALIDATION 44

6.1 Application de la démarche proposée 44

6.1.1 Préparation 44

6.1.2 Création de l'ISC 46

6.1.3 Atelier de validation 51

6.2 Validation des bases de l'ISC 52

6.3 Retours sur la démarche proposée 54

6.4 Recommandations 55

6.5 Suite du projet 57

CHAPITRE 7 CONCLUSION 59

RÉFÉRENCES 61

LISTE DES FIGURES

Figure 5.1 Positionnement des logiciels d'application dans l'organisation..... 29

Figure 6.1 Nombre d'outils de communication utilisés..... 48

Figure 6.2 Impacts de l'indisponibilité des principaux outils de communication par équipe 49

Figure 6.3 Informations sur l'utilisation de l'ERP..... 50

LISTE DES SIGLES ET ABRÉVIATIONS

La liste des sigles et abréviations présente, dans l'ordre alphabétique, les sigles et les abréviations utilisés dans le mémoire ou la thèse ainsi que leur signification.

BCI	Business Continuity Institute
BIA	Bilan d'Impact sur l'Activité
DMIA / DIMA	Durée d'Interruption Maximale Admissible
ERP	Enterprise Resource Planner
ISC	Image Situationnelle Commune
ODR	Objectif de Délais de Rétablissement
PCA	Plan de Continuité des Activités
PRI	Plan de Reprise Informatique
RPO	Point de récupération des données
SaaS	Software as a Service
TI	Technologies de l'Information
TIC	Technologies de l'Information et de la Communication
VPN	Virtual Private Network

LISTE DES ANNEXES

ANNEXE A Exemple de questionnaire pour les gestionnaires 65

ANNEXE B Exemple de questionnaires pour l'équipe TI 67

ANNEXE C Questionnaire pour l'exercice de validation 69

CHAPITRE 1 INTRODUCTION

Les avancées technologiques fulgurantes des dernières décennies ont permis l'adoption rapide de technologies numériques par les organisations, et ce dans la majorité des secteurs de l'économie (World Economic Forum, 2020). Ce rythme d'adoption a enregistré un bond significatif pendant la pandémie de COVID-19, alors qu'un grand nombre d'organisations ont été forcées de passer au télétravail (*COVID-19 digital transformation & technology | McKinsey*, s. d.) si bien qu'aujourd'hui, les technologies numériques sont omniprésentes dans la majorité des organisations (Statistiques Canada, 2024). Cette utilisation croissante s'accompagne toutefois d'une complexification inhérente de l'environnement technologique. L'interdépendance croissante entre les technologies (Sargut & McGrath, 2011), combinée à une gestion des systèmes souvent partiellement externalisée, crée un environnement intrinsèquement volatile et propice aux perturbations. Dans ce contexte d'évolution accélérée où chaque technologie progresse à son propre rythme, ces interdépendances, combinées à une gestion des systèmes souvent partiellement externalisée, rendent les perturbations non seulement plus fréquentes, mais aussi plus complexes à appréhender et à gérer. Alors que les incidents se multiplient et que les technologies numériques sont solidement ancrées dans les organisations, la vulnérabilité de leurs opérations face à l'utilisation de technologies numériques devient manifeste. Pour contrer cette menace de perturbations grandissante, les intervenants impliqués dans les stratégies de continuité des activités doivent impérativement développer une connaissance et une compréhension commune de l'environnement technologique et de son utilisation au sein de l'organisation — ils doivent se comprendre, collaborer efficacement et partager une vision unifiée des enjeux technologiques et opérationnels.

C'est dans cette optique que ce projet de recherche vise à développer une démarche structurée pour faciliter la collaboration entre ces intervenants. Notre approche est fondée sur l'établissement d'une connaissance approfondie et une compréhension commune de l'environnement technologique et de son utilisation au sein de l'organisation. Nous proposons d'atteindre cet objectif en développant une Image Situationnelle Commune (ISC), spécifiquement adaptée au contexte des organisations et aux technologies numériques qu'elles utilisent. Cette ISC permettra une meilleure appréhension des vulnérabilités opérationnelles découlant de l'usage des technologies numériques, renforçant ainsi la résilience organisationnelle.

Pour bien contextualiser les concepts abordés et guider le lecteur à travers notre démarche, cette recherche débutera par un état des connaissances, détaillant la structure et les caractéristiques des technologies numériques au sein d'une organisation, les perturbations qui peuvent les affecter, leur intégration dans les stratégies de continuité des activités, ainsi qu'une définition de la vulnérabilité. Cette base conceptuelle nous permettra ensuite de poser un constat précis, d'expliciter la problématique, de définir nos objectifs et de présenter la méthodologie employée pour cette recherche. Par la suite, nous aborderons les fondements de l'ISC dans un environnement technologique et proposerons une démarche concrète pour son élaboration. Nous expliquerons ensuite comment cette démarche concrète a été appliquée à une organisation, dans le cadre d'un exercice de validation, et présenterons l'analyse qui en a découlé. Enfin, nous terminerons en dégageant les grands principes, en formulant des recommandations pour de futures itérations et en synthétisant les apports de notre étude.

CHAPITRE 2 ÉTAT DES CONNAISSANCES

Ce chapitre vise à établir un état des connaissances des concepts qui sont au cœur de cette recherche et qui permettront de mieux comprendre et interpréter les résultats. Nous définirons d'abord les technologies numériques, leurs composantes et les perturbations qui peuvent les affecter. Ensuite, nous explorerons les méthodes employées par les organisations pour réduire l'impact de ces perturbations. Pour finir, les notions de vulnérabilité, ainsi que leur pertinence et application dans le cadre de cette recherche, seront explorées.

2.1 Comprendre les technologies numériques en contexte d'une organisation

Bien qu'il n'y ait pas de consensus sur la définition formelle du terme « technologie numérique », il fait généralement référence aux appareils, systèmes et ressources technologiques qui permettent aux utilisateurs de créer, de recueillir (stocker) ou de traiter (utiliser) des données (Banque de développement du Canada, 2022). Les technologies numériques se composent typiquement de logiciels d'application, de logiciels de système et d'équipements informatiques.

2.1.1 Logiciels d'application

Les technologies numériques qui sont dotées d'une interface utilisateur avec laquelle la majorité des acteurs d'une organisation peuvent interagir sont généralement nommées « logiciels d'application ». Ces logiciels sont utilisés pour accomplir des tâches qui ne sont pas directement liées au fonctionnement de l'équipement informatique ou aux ponts qui peuvent exister entre l'équipement informatique et l'interface utilisateur (« Application Software », 2025). Le logiciel d'application peut être installé sur un ordinateur ou être accessible via une architecture client-serveur, comme un navigateur web (DevX, 2023). Lorsqu'il est installé sur un ordinateur ou un appareil intelligent, le logiciel d'application peut fonctionner avec ou sans accès à internet. Par exemple, le logiciel d'application Outlook, qui est utilisé pour envoyer et recevoir des courriels, peut fonctionner, avec fonctionnalités réduites, sans accès à internet. L'utilisation des logiciels d'application est généralement très répandue au sein d'une organisation. Les logiciels de bureautique de type SaaS, qui servent généralement à faciliter et automatiser les tâches administratives et de gestion courante, comme les logiciels de la suite Microsoft Office ou de Google Workspace, en sont de bons exemples.

2.1.2 Logiciels de système

Les « logiciels de système » désignent les technologies numériques qui agissent comme intermédiaire entre l'infrastructure informatique (détaillée à la section 2.1.3) et les logiciels d'application. Ces logiciels fournissent un environnement permettant de créer, d'exécuter et de lancer les logiciels d'application (*What Is System Software?*, s. d.). Gérés pas l'équipe des technologies de l'information (TI), ils demeurent généralement invisibles pour les utilisateurs de logiciels d'application. Ce type de logiciel comprend par exemple les systèmes d'exploitation (OS ou Operating System) comme Linux ou Microsoft Windows. Les intergiciels (*middleware*) peuvent également être considérés comme des logiciels système. Ces logiciels tiers, comme par exemple comme IBM WebSphere ou Microsoft Azure Logic Apps, créent un réseau d'échange d'informations, sans intervention des utilisateurs, entre différentes applications informatiques hétéroclites (Red Hat, 2022).

2.1.3 Équipements informatique

Les logiciels d'application et de système sont entièrement dépendants des équipements informatiques qui leur permettent de fonctionner et d'être rendus disponibles aux utilisateurs par le biais de composants physiques généralement alimentés par électricité. Certains de ces composants physiques, tels qu'un ordinateur ou un téléphone intelligent, servent d'interface directe aux utilisateurs pour accéder aux logiciels d'application. Bien qu'il existe plusieurs termes pour désigner ce type d'appareils, nous utiliserons le terme « appareil utilisateur » dans le cadre de cette étude. Il existe un second type de composants physiques qui, invisibles à la majorité des utilisateurs, permettent aux logiciels d'être mis en service. On pense, par exemple, à un serveur, qui à lui seul contient une panoplie de composants physiques tels qu'un processeur, un disque dur ou une carte réseau. Nous nommerons ce type d'équipement « infrastructure informatique » dans le cadre de cette étude.

2.1.4 Prise en charge des technologies numériques

Un logiciel d'application ou de système peut être pris en charge par une équipe interne à l'organisation. Dans ce cas, le support aux utilisateurs, les interventions lors d'une interruption, la correction d'anomalies et l'ajout de fonctionnalités seront traitées par cette équipe interne, sans soutien majeur d'une partie tierce. On pourrait par exemple penser à une organisation qui aurait

développé son propre logiciel comptable afin de subvenir à ses besoins spécifiques, et qui hébergerait ce dernier sur son propre serveur. En contrepartie, le logiciel d'application ou de système peut être supporté par une équipe externe. Par exemple, une organisation peut avoir recours à des services de technologies de l'information (TI) externes si elle ne possède pas les connaissances nécessaires pour gérer une ou plusieurs des applications qu'elle utilise. Néanmoins, le cas de figure le plus répandu en matière de logiciels externalisés reste le SaaS. Le SaaS est un logiciel d'application basé sur l'infonuagique, pour lequel le fournisseur gère l'entièreté des ressources, physiques et logicielles, et garde le plein contrôle sur le logiciel et sa feuille de route. L'organisation y accède généralement en ligne, via un navigateur, par le biais d'un abonnement ou d'une licence, évitant ainsi l'achat du logiciel et l'installation locale. (Microsoft Azure, s. d.). Le support et les mises à jour du logiciel sont donc effectuées par le fournisseur. En raison de sa nature infonuagique, une connexion internet est généralement indispensable pour accéder à la pleine capacité de ce type de logiciel, même si certaines fonctionnalités limitées peuvent être disponibles hors ligne. Les logiciels d'application ou de système de type SaaS représentent environ 70 % de l'ensemble des logiciels utilisés par une organisation. Leur utilisation est répandue dans les organisations de toute taille : les organisations de 1 000 employés et plus utilisent en moyenne 177 applications de type SaaS, alors que les organisations de moins de 50 employés utilisent en moyenne 16 applications de type SaaS (BetterCloud, 2020). Au Canada, toutes les industries sont touchées par l'utilisation de SaaS, avec l'industrie des services en tête avec 41,3 % des répondants confirmant l'utilisation de SaaS dans leur organisation (Gouvernement du Canada, 2023). Les SaaS peuvent être utilisés pour accomplir une multitude de tâches, comme communiquer (par exemple Slack, Teams, Outlook), organiser le travail (par exemple Jira, Asana, Trello), concevoir (par exemple AutoCAD), déployer des efforts de vente (par exemple Salesforce) ou partager des documents (par exemple Dropbox ou Google Drive), pour ne nommer que quelques cas de figure.

Les bonnes pratiques recommandent que les SaaS soient préalablement autorisés par l'équipe TI avant d'en amorcer l'utilisation dans l'organisation (LeanIX, s. d.). Les contrats de service entre le fournisseur du SaaS et l'organisation devraient également être gérés par l'équipe TI. Cependant, dans la pratique, l'utilisation croissante des SaaS au cours des dernières décennies a contribué à l'augmentation d'un phénomène nommé *Shadow IT* ou *Grey IT*, qui désigne les actifs numériques qui sont utilisés dans l'organisation mais inconnus de l'équipe TI. Plus précisément, ce phénomène survient lorsqu'un individu ou une équipe décide d'utiliser un SaaS sans impliquer l'équipe TI. En

2022, on estimait qu'environ un tiers des SaaS utilisés dans les organisations n'étaient pas connus des équipes TI et qu'environ 30 % à 40 % des dépenses en SaaS dans une organisation étaient allouées à des SaaS pilotés directement par des équipes, sans l'approbation de l'équipe TI (*Spotlight on Shadow IT*, 2023). Alors qu'une équipe pourrait délibérément choisir d'utiliser une nouvelle plateforme SaaS pour contourner un problème spécifique, il est également possible que l'équipe ne soit pas consciente qu'elle utilise un nouveau SaaS. En effet, les SaaS proposent parfois des « connecteurs », des « extensions » ou des « apps » (le vocabulaire peut varier en fonction du SaaS) afin d'étendre les fonctionnalités du SaaS ou de permettre la connexion à d'autres systèmes. Or, ces extensions sont souvent des SaaS à part entière et l'équipe qui les active n'est pas systématiquement au fait de cette distinction. Finalement, il est à noter qu'il existe également des cas hybrides où la portion système d'un logiciel est supportée par une équipe interne tandis que la portion applicative est supportée par une équipe externe, ou vice versa.

Bien qu'il existe des exceptions, les appareils utilisateurs utilisés pour accéder aux logiciels sont en général détenus et pris en charge par l'organisation. Cependant, l'infrastructure informatique nécessaire au fonctionnement des logiciels peut être externalisée. En 2021, c'était déjà environ 60 % des actifs numériques des organisations qui étaient hébergés en infonuagique (Harvard Business Review, 2021), avec Amazon et Azure détenant respectivement 29 % et 22 % des parts du marché au premier trimestre de 2025 (Haranas, 2025). À l'heure actuelle, en infonuagique, il existe quatre grands modèles : *On-Premises*, *IaaS* (Infrastructure as a Service), *PaaS* (Platform as a Service) et *SaaS* (Software as a Service) (Jones, 2020). Ces modèles englobent une panoplie de cas de figure, en passant d'équipements informatiques détenus par l'organisation et entièrement géré par le département TI de l'organisation (modèle *On-Premises* ou parfois nommé *On-Prem*) jusqu'à des équipements informatiques entièrement détenus par des fournisseurs externes où le rôle de l'équipe TI se limite généralement à l'approbation des logiciels basée sur des standards de sécurité de l'organisation et à la gestion des contrats de services (modèle *SaaS*).

2.2 Perturbations des logiciels d'application

Le terme perturbation est généralement défini comme la « modification anormale du fonctionnement d'un mécanisme, du déroulement d'un processus » (Usito, s. d.). Dans le cas précis des technologies numériques, la perturbation se manifeste par une dégradation du service rendu par le logiciel ou l'équipement, l'empêchant ainsi de respecter ses spécifications, d'atteindre les

objectifs établis et d'offrir la performance attendue. Puisque cette étude est centrée sur la collaboration entre plusieurs équipes d'une organisation, nous nous attarderons uniquement aux manifestations des perturbations sur les logiciels connus et visibles par tous les intervenants d'une organisation, soit les logiciels d'application. Nous reviendrons sur ce point plus en détail au chapitre 5. Cette étude adoptera une approche globale qui se concentrera sur les impacts d'une perturbation des technologies numériques sur les opérations de l'organisation ; par conséquent, le détail des causes techniques des perturbations ne sera pas abordé.

2.2.1 Origine et ampleur

Puisque le fonctionnement des logiciels d'application est assuré par des systèmes tiers, la source de la perturbation peut contribuer à anticiper les impacts sur leur fonctionnement. À haut niveau, l'origine de la perturbation peut entrer dans les catégories suivantes :

- Panne de courant : ce type de panne affecte généralement tous les logiciels d'application puisque les appareils utilisateur et l'infrastructure informatique se retrouvent sans accès à l'électricité. Il est à noter que les pannes de courant sont en croissance. En effet, aux États-Unis, de 2018 à 2020, les coupures de courant ont représenté en moyenne 520 heures-clients par an. Au cours de cette période, 17 484 coupures ont duré plus de huit heures, tandis que 231 174 ont excédé une heure (Do et al., 2023). Pour les organisations, la croissance de ces pannes peut entraîner des pertes de productivité significatives et, ultimement, des coûts opérationnels accrus.
- Panne internet et problèmes de réseau : le nombre de logiciels d'application affectés par ce type de panne peut être variable, selon les logiciels d'application utilisés par l'organisation. Les logiciels d'application auxquels l'utilisateur accède à l'aide d'un navigateur web seront entièrement inaccessibles alors que d'autres logiciels d'application pourraient demeurer accessibles, avec des fonctionnalités réduites. Les logiciels d'application qui sont installés localement sur l'appareil de l'utilisateur, par exemple un logiciel de traitement de texte, peuvent demeurer entièrement fonctionnels.
- Panne de l'infrastructure informatique : le nombre de logiciels d'application affectés par ce type de panne peut être variable, selon le composant physique concerné. Par exemple, si la panne est liée à la température ambiante à l'intérieur d'une salle de serveurs, ce sont plusieurs serveurs qui pourraient se retrouver en panne au même moment, provoquant ainsi

la défaillance de nombreux logiciels d'application simultanément. Cependant, si le bris d'un composant physique provoque la défaillance d'un seul serveur, une portion plus limitée des logiciels d'application pourrait se retrouver affectée. Les pannes de l'infrastructure informatique peuvent survenir au sein de l'organisation ou chez un fournisseur, lorsque l'organisation n'est pas propriétaire de sa propre infrastructure informatique.

- Panne d'un logiciel de système : le nombre de logiciels d'application affectés par ce type de panne peut être variable. Comme il n'est pas rare qu'un seul logiciel de système assure le fonctionnement de plusieurs logiciels d'application, les impacts de la perturbation peuvent se faire sentir sur plusieurs logiciels à la fois, augmentant ainsi le nombre d'utilisateurs et d'activités affectées. Ce type de panne peut survenir dans l'organisation ou chez un fournisseur, lorsque l'organisation a externalisé certaines technologies numériques.
- Panne d'un logiciel d'application : le nombre de logiciels d'application affectés est généralement limité au logiciel d'application en question, à moins que celui-ci permette aux utilisateurs d'accéder à d'autres logiciels. Par exemple, dans plusieurs organisations, la connexion à un réseau privé, souvent via un logiciel d'application de type VPN (Virtual Private Network), peut être requise en télétravail, notamment pour des raisons de sécurité. Dans ce cas, certains logiciels d'application seront accessibles uniquement lorsque la connexion au réseau privé aura été établie. Dans ce contexte précis, si la panne affecte le logiciel d'application de type VPN, la perte d'accès au réseau privé empêchera l'utilisateur d'accéder à plusieurs autres logiciels. En 2021, alors que la pandémie de COVID-19 battait son plein et que le travail à distance était en croissance, l'utilisation d'un VPN (ou système similaire) en télétravail s'élevait à environ 43 % (PC Matic, 2021).

En 2022, 60 % des organisations ont rapporté avoir fait face à au moins une perturbation pendant l'année, avec 14 % de ces incidents qualifiés de sérieux. Des pannes internet et problèmes de réseau ont été la cause première de ces pannes avec 31 % des cas, suivis de près par les pannes de logiciels d'application ou de système, avec 28 % des cas. Quant à elles, les pannes électriques ont été la cause de 23 % des perturbations (Lawrence & Simon, 2023). Le coût d'une perturbation varie d'une organisation à l'autre. Bien qu'il n'y ait pas de consensus au niveau des coûts moyens par type d'organisation, les estimés se situent généralement entre 427 $ par minute pour une petite entreprise et jusqu'à 9 000 $ par minute pour une entreprise de taille moyenne (Atlassian, s. d.).

2.2.2 Manifestations des perturbations

Au niveau des logiciels d'application, les manifestations des perturbations peuvent se présenter de façons distinctes et comporter des caractéristiques propres à l'origine de la perturbation et à la nature du logiciel. Néanmoins, ces manifestations peuvent être regroupées en deux grandes catégories : la perte d'accès complète et l'utilisabilité partielle.

La perte d'accès complète survient lorsque l'utilisateur ne peut accéder au logiciel. Par exemple, pour un logiciel d'application accessible via un navigateur web, une page blanche ou un message d'erreur pourrait être affichés à l'adresse usuelle de l'application. Pour une application installée localement, la perte d'accès complète pourrait survenir lorsque l'utilisateur rencontre une erreur au démarrage, empêchant ainsi l'application de s'exécuter. Ce cas de figure peut également se produire lorsque l'appareil utilisateur utilisé pour accéder au logiciel n'est pas fonctionnel.

Un logiciel d'application présente une utilisabilité partielle lorsque l'utilisateur est en mesure d'y accéder mais que celui-ci ne rencontre pas l'ensemble de ses spécifications, objectifs ou requis de performance. Pour l'utilisateur, l'utilisabilité partielle peut se manifester de façons distinctes :

- Interface déficiente : l'utilisateur ne parvient pas à obtenir une compréhension visuelle suffisante de l'interface, il éprouve de la difficulté à se situer dans l'application, à comprendre les éléments graphiques de l'interface ou à déclencher certaines fonctionnalités. Par exemple :
    - Les sous-menus ne sont pas déclenchés lorsque l'utilisateur clique sur l'item menu de premier niveau et par conséquent, l'utilisateur n'est pas en mesure d'accéder à certaines sections secondaires de l'application.
    - Les éléments graphiques de l'écran se chevauchent et rendent certaines portions de l'interface illisibles.
- Fonctionnalités altérées : l'utilisateur peut accéder au logiciel d'application mais certaines fonctionnalités sont défectueuses. L'interface ne répond pas aux commandes de l'utilisateur ou ce dernier n'est pas en mesure de déclencher les actions désirées. Par exemple :
    - L'utilisateur n'est pas en mesure de sauvegarder les données.
    - Dans une liste de résultats, l'utilisateur n'est pas en mesure de filtrer ou réordonner les résultats.

- Connectivité : certaines fonctionnalités du logiciel d'application ne sont pas accessibles ou opérationnelles en raison d'une perte d'accès à internet ou à un manque au niveau d'un pont entre deux logiciels (*middleware*). Ce cas de figure s'applique surtout aux logiciels de type SaaS. Par exemple :
    - Dans une application de messagerie, l'utilisateur est en mesure de consulter l'historique de ses conversations, mais il n'est pas en mesure d'envoyer un nouveau message.
    - Les données les plus récentes n'ont pas été synchronisées ou ne sont pas synchronisées en temps réel.
- Performance dégradée : l'utilisateur peut accéder au logiciel d'application mais il fonctionne au ralenti, présente un temps de réponse inhabituellement long ou cesse de fonctionner de façon intermittente. Par exemple :
    - Après avoir saisi des données et enclenché la sauvegarde, l'utilisateur doit attendre un temps anormalement long pour consulter le résultat de la sauvegarde.
    - L'application affiche une page d'erreur à plusieurs reprises pendant l'utilisation.
- Compatibilité partielle : l'utilisateur peut accéder au logiciel d'application seulement sur certains appareils. Par exemple :
    - L'utilisateur peut accéder au logiciel d'application sur son ordinateur portable mais ne peut y accéder sur son téléphone intelligent.

2.3 Continuité des activités et reprise informatique

Dans une organisation, les technologies numériques se positionnent en support aux activités et processus qui lui permettent de produire ses biens et services. Le Business Continuity Institute (BCI) définit les activités comme « une ou plusieurs tâches entreprises par une organisation à l'appui d'un ou de plusieurs produits et services » et les processus comme un « ensemble d'activités corrélées ou interactives qui transforment des éléments d'entrée en éléments de sortie » (The Business Continuity Institute, 2018). Certaines activités sont naturellement plus prioritaires que d'autres, elles seront nommées « activités critiques » ou « activités prioritaires ». Ces dernières sont définies par le BCI comme des « activités auxquelles la priorité doit être donnée à la suite d'un incident afin d'en atténuer les impacts » (The Business Continuity Institute, 2018). Puisque les technologies numériques sont utilisées dans le cadre des activités et processus de l'organisation,

une perturbation de ces dernières peut produire des effets négatifs directs sur sa capacité à livrer ses produits ou services. Ultimement, ces impacts défavorables pourraient causer des pertes financières et empêcher l'organisation de remplir ses obligations contractuelles et légales, en plus de monopoliser le temps de plusieurs équipes, notamment l'équipe TI.

Afin de préparer leur réponse à toutes formes de perturbations, certaines organisations peuvent avoir mis en place des stratégies de continuité des activités. Bien que les perturbations à l'étude dans le cadre de ces dernières ne se limitent pas aux technologies numériques, 68,6 % des organisations listent tout de même la planification d'une réponse à une perturbation des actifs technologiques comme étant un des principaux résultats des stratégies de continuité des activités (The Business Continuity Institute, 2023). Dans la majorité des organisations, la mise en place de stratégies de continuité des activités passe par la création d'un Plan de Continuité des Activités (PCA) et d'un Plan de Reprise Informatique (PRI). Alors que le PCA vise à fournir un guide pour répondre aux perturbations de façon générale, le PRI se concentre spécifiquement sur la remise en service des technologies numériques. Afin de mieux situer les technologies numériques dans l'univers des stratégies de continuité des activités, cette section détaillera la façon dont celles-ci sont prises en compte dans le PCA et le PRI.

2.3.1 Plan de continuité des activités

Le BCI définit le PCA comme des « procédures documentées servant de guide aux organisations pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation » (The Business Continuity Institute, 2018). Le PCA n'est pas exigé dans toutes les organisations. Au Québec, en 2018, c'était uniquement 52 % des moyennes et grandes entreprises qui disposaient d'un PCA (Gouvernement du Québec, 2018). Le développement et la mise à jour du PCA sont généralement pris en charge par l'équipe de continuité opérationnelle ou l'équipe des opérations, lorsque l'organisation ne dispose pas d'équipe de continuité opérationnelle dédiée. En 2023, parmi les organisations qui avaient déjà mis en place des stratégies de continuité des activités, seulement 50 % disposaient d'une équipe dédiée à la continuité opérationnelle (The Business Continuity Institute, 2023). Bien que la composition d'une équipe de continuité opérationnelle varie grandement d'une organisation à l'autre, elle comprend généralement un responsable du PCA, une équipe de planification et de gestion. L'équipe de continuité doit travailler en étroite collaboration avec des représentants des équipes opérationnelles que nous nommerons

« gestionnaires » dans le cadre de cette recherche. Il n'existe généralement pas de lien hiérarchique entre l'équipe de continuité et les gestionnaires. Quant à l'équipe des opérations, sa composition varie grandement selon la taille, le marché et les produits ou services de l'organisation, mais en général, l'équipe est au minimum constituée d'un directeur des opérations qui peut être entre autres chargé de superviser les gestionnaires de chaque équipe et s'assurer d'améliorer la qualité des produits, la productivité et les performances de l'organisation. Dans le cadre de cette recherche, par souci de simplification, nous utiliserons le terme « équipe de continuité » pour désigner l'équipe chargée de la continuité opérationnelle dans une organisation, qu'elle soit une équipe à part entière ou qu'elle soit partie intégrante de l'équipe des opérations.

Dans le cadre du développement du PCA, le Guide de bonnes pratiques du BCI recommande que l'organisation identifie ses activités et processus critiques et explore les effets d'une perturbation sur ces derniers, via un ou plusieurs exercices de bilans d'impact (BIA ou *Business Impact Analysis*). L'organisation peut choisir d'effectuer un premier BIA afin d'identifier ses produits ou services prioritaires et par la suite enchaîner avec des BIA plus granulaires qui lui permettront de déterminer les processus et activités qui supportent les produits et services prioritaires. Il est à noter que certaines organisations choisiront de ne pas effectuer tous les niveaux de BIA ; la taille de l'organisation, la complexité des processus et les efforts alloués aux stratégies de continuité des activités en seront des facteurs déterminants. Néanmoins, c'est par l'entremise du BIA que l'organisation pourra prioriser les activités jugées prioritaires pour assurer le maintien en cas de perturbation.

Les données servant de base aux BIA seront généralement recueillies par le biais d'ateliers, de questionnaires et d'entretiens auprès des individus ou équipes impliquées dans les processus ou activités considérées. Au niveau des activités jugées critiques pour l'organisation, cette démarche permettra d'établir une Durée maximale d'interruption acceptable (DMIA, ou parfois DIMA) pour chaque activité considérée, soit le « temps nécessaire pour que les impacts défavorables pouvant résulter de la non-fourniture d'un produit/service ou de la non-réalisation d'une activité, deviennent inacceptables » (The Business Continuity Institute, 2018). Une liste de ressources requises, parmi lesquelles certains logiciels d'application peuvent figurer, pour accomplir chaque activité à la suite d'une perturbation, sera également créée. Pour chacun de ces logiciels d'application, un objectif de délai de rétablissement (ODR, ou parfois RTO), soit la « durée après un incident durant laquelle des ressources doivent être rétablies » (The Business Continuity Institute, 2018), sera fixé en

contexte de chaque activité et ce, en prenant en compte la tolérance à l'interruption, soit la valeur DMIA, de l'activité. Chaque logiciel d'application listé disposera également d'une valeur de point de récupération des données (RPO) soit le « point à partir duquel les informations utilisées par une activité doivent être restaurées afin de permettre son fonctionnement ou rétablissement » (The Business Continuity Institute, 2018). Certains logiciels sont utilisés dans le cadre de plusieurs activités critiques, on pense par exemple à un logiciel ERP (Enterprise Resource Planner) qui peut être employé pour la comptabilité, la gestion d'inventaire et les achats, pour ne nommer que quelques exemples. Dans ce cas, des valeurs ODR et RPO seront attribuées au logiciel en contexte de chaque activité critique dans lequel ce dernier est utilisé. Ces valeurs seront ensuite comparées d'une activité à l'autre et ce sont les valeurs les plus courtes, donc les valeurs qui représentent les objectifs les plus agressifs, qui seront attribuées au logiciel dans le PCA.

En plus des logiciels d'application, la liste des ressources requises à la suite d'une perturbation contient généralement les appareils utilisateurs, comme des ordinateurs ou des téléphones intelligents, qui permet d'accéder à ces derniers. Une liste des fournisseurs de services ou partenaires d'affaires indispensables sans lesquels les activités critiques ne pourraient être menées à terme à la suite d'une perturbation sera également dressée. Cette liste pourrait contenir certains fournisseurs de technologies numériques et dans ce cas, elle sera accompagnée des modalités sommaires de l'entente de service, si applicable.

2.3.2 Plan de reprise informatique

Le PRI vise à assurer la reprise des services TI qui appuient les activités de l'organisation. Au minimum, le plan doit contenir les processus, les applications et les données qui sont essentielles, et expliciter la façon dont l'organisation pourra assurer la reprise des services TI en cas de perturbation (Centre canadien pour la cybersécurité, 2021). Généralement, le PRI contient une liste des clients internes et des fournisseurs de services. Alors que les logiciels listés dans le PCA sont généralement des logiciels d'application, le PRI prend également en compte les logiciels de système et les équipements informatiques. Souvent, le PRI comprend aussi un schéma de réseau inventoriant l'ensemble des technologies numériques, leurs interdépendances et leurs modalités de prise en charge, par des équipes internes ou par des parties tierces.

Dans une organisation, le PRI est généralement développé et mis à jour par l'équipe TI. Bien que la composition de l'équipe TI varie d'un contexte technologique à l'autre, elle est généralement

chargée de gérer, maintenir et optimiser les technologies numériques de l'organisation. Dans la plupart des cas, l'équipe TI est majoritairement composée de rôles qui nécessitent une formation technique. Par exemple, dans les équipes TI de la fonction publique québécoise, les rôles strictement techniques représentaient environ 90 % du total en 2015 (Gouvernement du Québec, 2016). Certaines organisations peuvent avoir créé un rôle spécifique pour gérer la continuité des activités au sein de l'équipe TI, mais pour d'autres, ce rôle sera partagé entre différents membres de l'équipe. Certaines organisations pourront également choisir d'externaliser le PRI (service DRaaS ou Disaster-Recovery-as-a-Service).

Le PRI n'est pas exigé dans toutes les organisations. En effet, en 2021, alors que 66 % des organisations avaient dédié des ressources pour mieux comprendre leurs vulnérabilités, seulement 20 % des organisations possédaient un PRI formel (Faivre, 2021).

2.3.3 Points d'intersection

Le PCA et le PRI se complètent et se recoupent à plusieurs niveaux. Lorsqu'un logiciel d'application est considéré comme une ressource requise dans le cadre d'une activité critique du PCA, il doit également être considéré comme critique dans le PRI. Il s'ensuit que le PRI et le PCA doivent être alignés au niveau des objectifs de délai de rétablissement (ODR) et de point de récupération des données (RPO), et ce, pour les appareils utilisateurs, les logiciels d'application et de système ainsi que pour l'infrastructure informatique, dans un contexte d'interdépendance. Un recoupement d'informations peut également être constaté au niveau de la liste des fournisseurs de services. Alors que le PCA aura permis de dresser une liste des fournisseurs de logiciels d'application, le PRI devra également répertorier les fournisseurs de logiciels de système, d'appareils utilisateurs et d'infrastructure informatique, ainsi que compléter certaines informations de prise en charge des logiciels. En revanche, si un logiciel est utilisé par une équipe et non répertorié par l'équipe TI (phénomène de *Shadow IT*), ce dernier sera uniquement répertorié au niveau du PCA.

Le PCA et le PRI présentant plusieurs recoupements d'informations, les gestionnaires, l'équipe de continuité et l'équipe TI seront appelés à collaborer pour s'assurer que les informations pertinentes sont partagées, transmises et intégrées dans les plans respectifs.

2.3.4 Prise en charge des perturbations

En cas de perturbation des technologies numériques, l'équipe chargée d'investiguer et de rétablir le service dépendra de l'origine et de l'ampleur de la perturbation, des logiciels affectés ainsi que des contrats de services entre l'organisation et ses fournisseurs de service, si certaines technologies numériques ont été externalisées. En effet, comme exploré à la section 2.1.4, il est fréquent que les organisations externalisent certaines de leurs technologies numériques et que la responsabilité de leur prise en charge soit partagée entre plusieurs équipes. En 2022, 42 % des perturbations rapportées par les organisations étaient attribuables à des services tiers ou externalisés (Lawrence & Simon, 2023). Dans ce contexte, la prise en charge des problèmes ou anomalies, la coordination et la communication entre les équipes qui peuvent se retrouver dans des fuseaux horaires différents peuvent s'avérer complexes.

2.4 Notions de vulnérabilité

Le terme « vulnérabilité » est utilisé dans plusieurs disciplines, telles que l'économie, la politique, la sociologie, la psychologie, la biologie, l'environnement, l'urbanisme et l'informatique. Sa définition peut varier en fonction du contexte, de l'objet ou du système qu'il décrit. Par exemple, en sciences de l'environnement, le terme est décrit comme l'état de susceptibilité aux dommages causés par l'exposition aux stress associés aux changements environnementaux et sociaux (Adger, 2006) tandis qu'en urbanisme, le terme est généralement défini comme la capacité d'un système à être endommagé ou abîmé par un stress ou une perturbation (Suarez, 2002). De façon plus générale, le terme exprime une prédisposition ou susceptibilité d'un système, d'un objet ou d'une personne à être affectée ou endommagée à la suite de l'exposition à un aléa (Cardona, 2004). En contexte de la continuité des activités, le Guide des Bonnes Pratiques du BCI, bien qu'il n'aborde pas la vulnérabilité explicitement, adopte une approche stratégique et globale en exhortant les organisations à identifier les menaces et à concevoir des solutions pour réduire la probabilité d'incidents ou en minimiser les impacts. Ces solutions peuvent inclure des mesures d'atténuation ou de repli qui ciblent directement les technologies numériques. La collaboration étroite avec les professionnels de la sécurité de l'information de l'équipe TI pour développer et mettre en œuvre ces solutions est alors encouragée.

En informatique, le terme « vulnérabilité » revêt une définition encore plus spécifique. Il est généralement employé pour décrire l'état de faiblesse d'un logiciel d'application ou d'un logiciel

de système se traduisant par une incapacité partielle de celui-ci à faire face aux attaques (Office de la langue française, s. d.). Dans ce contexte, l'état de faiblesse est induit par une ou plusieurs failles pouvant découler d'une panoplie de facteurs : des erreurs durant la conception d'un logiciel, des mauvaises configurations des systèmes et des réseaux, une mauvaise gestion des identités et des accès, une obsolescence des logiciels et de l'équipement, et même des facteurs humains, comme des erreurs ou mauvaises manipulations du côté des utilisateurs. Les attaques se présentent sous forme d'une exploitation potentielle de ces failles, compromettant ainsi la sécurité et la stabilité des technologies numériques (Dempsey et al., 2019). Comme expliqué à la section 2.1.4, la responsabilité de prévenir, d'investiguer et de remédier aux vulnérabilités informatiques peut être partagée entre l'équipe TI et les fournisseurs de logiciels et de services de l'organisation, selon la nature et la structure des technologies numériques de l'organisation. Par exemple, si l'organisation fait l'utilisation d'un SaaS et qu'une vulnérabilité y est découverte, c'est généralement le fournisseur du SaaS qui prendra en charge la vulnérabilité. En cas de perturbation, c'est principalement à l'équipe TI de l'organisation qu'il incombera d'analyser les impacts sur les données et la sécurité, puis de prendre des mesures supplémentaires, telles qu'effectuer des mises à jour ou communiquer de l'information aux utilisateurs. Le PRI, qui présente une approche plus opérationnelle et technique que le PCA, détaillera généralement ces modalités de prise en charge ainsi que le plan d'action nécessaire pour rétablir le service.

Alors que la vulnérabilité informatique est un concept compris et accepté dans le domaine des technologies, il reste limité à l'identification des failles techniques, à l'analyse des impacts sur les technologies numériques et aux mesures d'atténuation techniques. Afin d'offrir une perspective sur la vulnérabilité qui soit plus large, cette recherche propose d'étudier la vulnérabilité des opérations de l'organisation face à son utilisation des technologies numériques. Dans ce contexte, le terme « opérations » désigne l'ensemble des activités et processus quotidiens liés à la gestion de l'organisation (Banque de développement du Canada, s. d.). Nous proposons de définir ce type de vulnérabilité comme la prédisposition des activités et processus d'une organisation à être affectées par une perturbation de ses technologies numériques. Alors que la « vulnérabilité informatique » s'intéresse principalement à l'impact de l'exploitation d'une faille sur les technologies numériques, la « vulnérabilité de l'organisation face à son utilisation de technologies numériques » s'intéresse plutôt aux impacts d'une perturbation des technologies numériques sur les opérations de l'organisation. Dans l'optique de ce type de vulnérabilité, les menaces se manifestent par

l'altération potentielle des services rendus par les technologies numériques dont les activités dépendent. C'est, en d'autres termes, l'incapacité de l'organisation à exécuter normalement ses tâches et processus parce que les technologies numériques qui y sont nécessaires sont dégradés ou inopérants. Ce type de vulnérabilité, bien qu'il puisse parfois être implicitement compris par certains intervenants, notamment par l'entremise du PCA et du PRI, n'est pas systématiquement formalisé et communiqué à tous les intervenants impliqués dans les stratégies de continuité des activités.

CHAPITRE 3 CONSTATS

La conjoncture technologique, combinée à l'utilisation croissante des technologies numériques dans les organisations, rend leurs opérations vulnérables aux perturbations. Dans ce contexte, une collaboration étroite et une compréhension mutuelle entre les gestionnaires, l'équipe de continuité et l'équipe TI sont essentielles pour appréhender cette vulnérabilité et assurer une préparation adéquate de l'organisation aux perturbations. Pourtant, notre expérience professionnelle des dix dernières années en tant que point de contact stratégique entre des équipes opérationnelles et techniques nous a permis de faire un constat plus nuancé : les activités entourant l'élaboration et le maintien de stratégies de continuité des activités ne suffisent pas à établir une connaissance et une compréhension commune de l'environnement technologique et de son utilisation au sein de l'organisation, entre les gestionnaires, l'équipe de continuité et l'équipe TI. Alors que la majorité des intervenants d'une organisation ont une compréhension des technologies numériques axée sur l'utilisation de logiciels d'application spécifiques, la compréhension des intervenants de l'équipe TI est axée sur l'aspect technique du système, incluant l'infrastructure informatique, les logiciels de système, les logiciels d'application et les appareils utilisateurs. L'équipe TI, qui considère les technologies numériques comme ses principaux produits, éprouve souvent des difficultés à en communiquer la complexité et les limites. De leur côté, les gestionnaires et l'équipe de continuité, percevant les technologies numériques comme des outils, se soucient surtout de la disponibilité et du bon fonctionnement des logiciels d'application. Dans le cadre de l'élaboration et du maintien des stratégies de continuité des activités telles que présentées à la section 2.3, ce manque d'alignement relativement à l'utilisation, aux limites et à la complexité des technologies numériques peut mener à une collaboration épineuse entre les intervenants. Pour aggraver la situation, et comme exploré à la section 2.3, la diversité des champs de compétences des intervenants impliqués offre peu de points d'intersection et complexifie davantage l'échange d'informations. En effet, alors que les gestionnaires utilisent un vocabulaire axé sur les opérations et les réalités de leur équipe, l'équipe de continuité a son propre jargon et ses acronymes, et l'équipe TI emploie une terminologie technique. Sur le terrain, nous constatons également une implication souvent insuffisante de l'équipe TI pendant la création du PCA, ce qui creuse davantage le fossé entre les équipes. En effet, sans la participation de l'équipe TI, l'équipe de continuité est forcée d'élaborer des mesures d'atténuation ou de repli sans l'apport et la validation de l'équipe TI. De son côté, l'équipe TI pourra éventuellement se retrouver dans une position où elle devra répondre

à des exigences de disponibilité de logiciels, via les valeurs ODR et RPO explorée à la section 2.3.1, sans avoir eu la chance de participer au processus de création des requis ou de se prononcer sur la faisabilité technique.

Bien que le développement de stratégies de continuité des activités puisse offrir une opportunité de collaboration pour les équipes, dans les faits, les activités entourant la création du PCA et du PRI telles que nous les avons explorées à la section 2.3, ne favorisent pas la mise en commun et la synthèse d'informations. Ceci s'explique en partie par le fait que, comme spécifié à la section 2.3.2, les résultats du BIA, utilisés comme base pour le PCA, ne permettent de couvrir que les technologies numériques liées aux activités critiques, négligeant potentiellment plusieurs logiciels d'application dont l'utilisation s'avère répandue dans l'organisation. On pense, par exemple, à un logiciel d'organisation de tâches qui est généralement utilisé pour planifier, détailler, assigner et suivre l'avancement du travail : bien qu'il puisse ne pas être directement lié à une activité critique pour l'accomplissement de son objectif principal, il peut être essentiel à de multiples activités ou tâches de soutien. Même pour une activité critique, certains logiciels — par exemple un logiciel pour communiquer entre les équipes — parfois considérés comme accessoires, pourraient avoir été oubliés ou laissés de côté dans le BIA. Il en résulte que certains logiciels permettant aux équipes de travailler ensemble ne sont pas systématiquement recensés pendant le BIA, qu'ils ne sont pas inclus au PCA, et que, par conséquent, aucune solution de repli n'est identifiée. Bien que certains de ces logiciels puissent avoir été recensés, schématisés et explicités par l'équipe TI par l'entremise du PRI, les informations ne seront pas nécessairement complètes en termes d'utilisation, ni formulées de façon à être comprises par les gestionnaires ou les intervenants de l'équipe de continuité. Il en résulte qu'il sera difficile de consolider, réconcilier et d'harmoniser l'information entre le PCA et le PRI et que l'utilisation réelle des technologies numériques dans l'organisation pourra demeurer méconnue.

En plus de présenter des lacunes quant aux informations d'utilisation des technologies numériques, la création du PCA offre une évaluation sommaire de l'importance des logiciels critiques, sans toutefois fournir de détail crucial sur le type d'utilisation qui en est fait. Comme exploré à la section 2.3.2, l'organisation aura pu recenser les logiciels d'application nécessaires à ses activités critiques grâce au BIA. Cette information, combinée à la valeur de DMIA attribuée à chaque activité critique, pourra offrir une évaluation intrinsèque de l'importance de chaque logiciel d'application qui supporte les activités critiques de l'organisation. Si la valeur de DMIA pour une activité est courte

et que cette activité requiert un logiciel d'application particulier, l'organisation pourra pressentir l'importance du logiciel d'application dans ses opérations. Cependant, sans analyse supplémentaire, cette analyse informelle demeure isolée et incomplète ; elle ne permet pas de comprendre les détails de l'utilisation du logiciel dans l'activité en question ou dans les autres activités qui n'auront pas été déterminées critiques. De plus, puisque l'exercice BIA ne requiert pas de décrire le type d'utilisation qui est fait du logiciel, il ne sera pas non plus possible d'anticiper la nature des impacts sur les opérations de l'organisation en fonction du type et de l'ampleur d'une perturbation des technologies numériques. Par exemple, un logiciel de travail collaboratif, comme Google Sheets ou Excel (via OneDrive), pourrait avoir été listé comme nécessaire à une activité critique. Cependant, le logiciel peut être utilisé à plusieurs fins : pour obtenir des données, pour communiquer, pour visualiser des données ou pour partager des données avec d'autres systèmes. Si la perturbation survient au niveau de la connectivité du logiciel, les données pourraient être consultées, mais elles ne pourront pas être rafraîchies. Dès lors, dans un cas où l'activité critique nécessite la consultation de données statiques, une perturbation de type utilisabilité partielle sans connectivité pourrait être acceptable. À l'opposé, si des données dynamiques sont nécessaires pour consultation par l'utilisateur ou consommation par d'autres logiciels, la perturbation déclencherait des problèmes immédiats. Il n'est donc pas possible de prédire comment l'activité sera affectée par la perturbation du logiciel d'application. Bien que le PRI puisse fournir certains indices sur l'utilisation de logiciels d'application sous forme de spécifications techniques, on n'y retrouve pas les détails d'utilisation nécessaires pour anticiper les impacts d'une perturbation.

En conclusion, au-delà d'offrir une perspective incomplète sur l'utilisation des technologies numériques dans l'organisation, nous constatons que le processus de création et de maintien du PCA et du PRI n'offre pas aux intervenants l'opportunité de réconcilier les informations et d'établir des points de référence communs. Plus simplement dit, bien qu'ils regorgent de détails techniques dans leurs sphères d'application respectives, le PCA et le PRI n'aident pas les intervenants à mieux se comprendre. En théorie, le PRI, bien qu'il offre un portrait limité au contexte technique, pourrait bonifier certaines informations recueillies pendant le développement du PCA. Cependant, en pratique, étant donné leur spécificité et leurs objectifs distincts, la simple existence des deux plans ne garantit pas une connaissance et une compréhension commune de l'environnement technologique et de son utilisation dans l'organisation.

CHAPITRE 4 CADRE ET DÉMARCHE DE RECHERCHE

Ce chapitre établit les fondements conceptuels et la méthodologie de cette étude. Nous y présenterons le cadre théorique qui guide notre réflexion, notamment le concept d'unité d'effort et sa pertinence pour améliorer la collaboration entre les gestionnaires, l'équipe de continuité et l'équipe TI. Nous explorerons également le rôle central joué par l'Image Situationnelle Commune (ISC) pour soutenir cette unité d'effort dans un contexte de préparation aux perturbations des technologiques numériques dans l'organisation, comme outil pour améliorer la connaissance et la compréhension de ces technologies et de leur utilisation. Ensuite, nous détaillerons les objectifs spécifiques de notre recherche. Enfin, nous exposerons la méthodologie recherche-design adoptée, expliquant comment cette approche itérative et collaborative nous a permis d'explorer le problème, de développer des outils concrets et de valider nos propositions sur le terrain.

4.1 Cadre de la recherche

Cette recherche s'inscrit dans le cadre de recherches menées par le Centre risque & performance dans lesquelles le concept d'unité d'effort est adapté à un contexte de préparation à des perturbations dans des organisations, dans le but d'améliorer la collaboration entre des intervenants. L'objectif premier de l'unité d'effort est de garantir qu'en situation d'urgence, un large éventail d'intervenants puissent coordonner leurs ressources efficacement et se concentrer sur un objectif commun (U.S. Air Force, 2021). Bien que le concept ait trouvé son origine dans un contexte militaire, dans une optique de coopération et de collaboration lors d'opérations complexes, Micouleau (2023) confirme son applicabilité à une situation d'urgence dans une organisation, en particulier lorsque plusieurs équipes sont appelées à prendre des décisions et à poser des actions de façon synergique. Allant plus loin, Mercier Aubin (2025) et Gilbert Roussel (2024) démontrent par la suite que le concept peut être élargi et appliqué à la gestion courante, dans un contexte de préparation à des perturbations. Ces travaux soulignent l'efficacité de l'unité d'effort pour établir des bases de collaboration en renforçant la compréhension commune de l'environnement, particulièrement lorsque des intervenants sans liens hiérarchiques n'ont pas l'habitude de collaborer dans le cadre de leurs fonctions.

Micouleau (2023) met en évidence le rôle de l'ISC dans l'établissement de la compréhension commune de l'environnement, essentielle à l'unité d'effort. L'ISC repose sur l'Image Situationnelle (IS) qui est définie comme « la perception des éléments de l'environnement et la

compréhension de leur signification, pouvant inclure une projection de l'état futur des éléments perçus et du risque associé à cet état » (*ISO 17757:2019*, 2019). Comme résumé par Mercier-Aubin (2025), l'IS se construit à travers trois niveaux :

- La perception des éléments dans l'environnement : ce premier niveau consiste à identifier les éléments pertinents de la situation étudiée. Le défi est de filtrer l'information pour ne retenir que ce qui est essentiel à la compréhension, sans analyse approfondie.
- La compréhension de la situation actuelle : ce deuxième niveau vise à donner du sens à l'information collectée, en l'interprétant en fonction des buts et objectifs définis.
- La projection dans le futur : ce troisième et dernier niveau permet d'anticiper les évolutions futures de la situation en se basant sur la perception et la compréhension actuelles.

l'ISC prend forme lorsque les informations de différentes sources sont mises en commun, synthétisées, puis visualisées et comprises par tous les intervenants impliqués. Même si traditionnellement le concept d'IS a été majoritairement appliqué dans un contexte d'intervention ou d'urgence, les travaux de Gilbert Roussel (2024), Mercier Aubin (2025) et Charmont (2025) confirment la pertinence de l'ISC comme outil de support à l'unité d'effort en gestion courante. Dans les travaux de Mercier Aubin (2025), dans un contexte de préparation à des situations d'urgence dans le milieu hospitalier, l'ISC prend la forme de tableaux synthétisant les informations critiques, pour ainsi offrir aux intervenants une vision globale des ressources nécessaires dans un contexte de perturbation. Dans les travaux de Gilbert Roussel (2024) et Charmont (2025), dans un contexte de vulnérabilité face à l'électricité, l'ISC est créée à partir d'informations obtenues via des questionnaires sur les impacts d'une perturbation, ces données étant ensuite consolidées et présentées dans un format graphique. Dans les trois cas, l'ISC identifie et dégage les informations pertinentes dans un format clair, permettant ainsi à tous les intervenants de les visualiser et de les comprendre.

Pour faire suite à ces travaux, la présente étude s'intéresse à l'application du concept d'unité d'effort pour soutenir la collaboration entre les gestionnaires, l'équipe de continuité et l'équipe TI, dans le cadre de la préparation de l'organisation aux perturbations de ses technologies numériques, soit la création et la mise à jour de stratégies de continuité des activités. Ce contexte présente des défis particuliers qui renforcent la nécessité de cette collaboration proactive. En effet, comme présenté au chapitre 2, la nature dynamique des technologies numériques, marquée par l'adoption

continue et rapide de nouveaux outils, l'évolution technologique et les changements d'habitudes des utilisateurs, exacerbe la fréquence des perturbations. À cela s'ajoute la complexité inhérente des technologies numériques, due entre autres au nombre et à l'interdépendance des logiciels. Dans cet environnement en constante évolution et nécessitant une réponse perpétuelle aux perturbations, l'unité d'effort est donc particulièrement pertinente. De plus, le contexte de préparation aux perturbations, comme exploré au chapitre 2.3, implique des intervenants aux expertises très variées qui, de surcroît, ne possèdent pas de lien hiérarchique direct. Comme expliqué au chapitre 3, cette situation conduit souvent à une collaboration limitée. Il est à noter que contrairement au concept original d'unité d'effort développé dans le milieu militaire, l'approche proposée dans le cadre de cette recherche n'est pas limitée à une situation de perturbation. Elle est plutôt permanente, comme suggéré par les travaux de Mercier Aubin (2025), et vise à soutenir la collaboration continue en contexte de préparation à des perturbations. Puisque l'efficacité de l'ISC pour établir une connaissance et une compréhension commune de l'environnement et soutenir l'unité d'effort a été démontrée dans les travaux de Gilbert Roussel (2024), Mercier Aubin (2025) et Charmont (2025) nous proposons de l'utiliser comme outil clé pour soutenir l'unité d'effort proposée dans le cadre de cette recherche.

4.2 Objectifs de la recherche

Cette recherche a pour but de proposer des mécanismes qui permettent d'améliorer la collaboration entre les gestionnaires, l'équipe de continuité et l'équipe TI, grâce à une connaissance et une compréhension commune de l'environnement technologique et de son utilisation dans l'organisation. Pour atteindre cet objectif général, les sous-objectifs suivants ont été déterminés :

- Définir et valider les dimensions d'une ISC qui favorisent la compréhension commune de l'environnement technologique et de son utilisation ;
- Proposer une démarche pour renforcer la collaboration dans le contexte de préparation à des perturbations des technologies numériques ;
- Tester et valider cette démarche auprès d'une organisation ;
- Proposer des recommandations et dégager des principes de design pour améliorer cette démarche.

4.3 Méthodologie

La nature concrète et contextualisée des objectifs de recherche nous a conduit à privilégier la méthodologie recherche-design. Définie par Wang et Hannafin (2005, p.2) comme étant systématique et flexible, cette méthodologie de recherche a pour objectif d'améliorer les pratiques en procédant à des phases d'analyse, de conception, de développement et de mise en œuvre, s'appuyant sur une collaboration étroite entre chercheurs et praticiens en milieu réel. Cette méthodologie de recherche, axée sur l'approche terrain et la collaboration, est donc particulièrement adaptée à ce projet dont l'objectif principal consiste à amener des équipes à améliorer la collaboration en forgeant une compréhension commune de leur environnement technologique et de son utilisation. L'efficacité de cette méthode a d'ailleurs été confirmée par Mercier Aubin (2025) dans le cadre d'un projet aux visées similaires, où il s'agissait d'améliorer la collaboration de différents intervenants d'une organisation du milieu hospitalier, par le développement d'une unité d'effort basée sur une ISC.

Cette étude s'appuie sur les constats explorés au chapitre 3, lesquels découlent d'expériences professionnelles en tant que point de contact principal pour des équipes technologiques. Grâce à cette expérience, acquise sur plusieurs années et dans de multiples secteurs, nous avons constaté que la connaissance de l'environnement technologique et de son utilisation dans une organisation est souvent hétérogène et que la collaboration entre les équipes participant à la mise en œuvre de stratégies de continuité des activités est insuffisante. C'est cette analyse des milieux de travail qui nous permis de formaliser le constat présenté au chapitre 3 ainsi que les objectifs de ce projet de recherche.

Cette même expérience professionnelle nous a également permis d'identifier et de détailler une portion clé des technologies numériques pouvant servir de base à l'ISC. Cette portion clé a ensuite été décomposée en dimensions, définies à partir de connaissances des technologies et de nos constats initiaux. Pour valider ces dimensions et dégager des lignes directrices applicables aux itérations futures, nous avons organisé un atelier, amorçant ainsi le cycle itératif de la méthode recherche-design. Cet atelier a rassemblé environ 60 professionnels de la continuité des activités, issus de secteurs variés tels que la santé, la finance, l'énergie, le manufacturier et les TI. Les échanges avec et entre les participants nous ont permis de confirmer la pertinence des dimensions

proposées pour la plupart des secteurs. La portion clé des technologies numériques sélectionnée ainsi que les dimensions de l'ISC proposées seront détaillées au chapitre 5.

Alors que plusieurs techniques sont envisageables pour créer l'ISC, Gilbert Roussel (2024) a démontré qu'elle peut être créée par la synthèse et visualisation d'information provenant de questionnaires qui comprennent des questions informatives ainsi que des questions menant les intervenants à poser des jugements professionnels. Comme le souligne le CVIIP (2011, p. 40), le jugement professionnel est une conclusion limitée par l'étendue de l'expérience et des compétences du praticien. Dans une approche similaire à celle de Gilbert Roussel (2024), nous avons élaboré une première version de l'ISC en combinant et consolidant les jugements professionnels des gestionnaires et les informations techniques et opérationnelles fournies par l'équipe TI, le tout recueilli sur la base de nos dimensions. Ces informations ont par la ensuite été synthétisées et illustrées sous forme de figures.

Mercier Aubin (2025), Gilbert Roussel (2024) et Charmont (2025) démontrent tous les trois que la validation de l'ISC permet de la solidifier et, par extension, de renforcer la collaboration qui est partie intégrante de l'unité d'effort. En effet, c'est au fil de ce processus de validation que les intervenants sont amenés à enrichir leurs connaissances, instaurer un langage commun et former une compréhension cohérente de l'environnement technologique de l'organisation. C'est ainsi que, basée sur nos constats initiaux, les conclusions de l'atelier auquel nous avons participé et les recherches du Centre risque & performance, nous avons été en mesure de formaliser notre démarche pour initier une approche collaborative basée sur la création et la validation de l'ISC. Nous avons ensuite été en mesure de valider cette démarche auprès d'une organisation.

Ces premières itérations de la méthodologie recherche-design nous ont permis de tirer des conclusions, d'émettre des recommandations et d'extraire des principes de design applicables aux itérations futures. C'est en s'appuyant sur ces recommandations que ce cycle pourrait être répété à plusieurs reprises, dans une perspective d'approfondissement, afin de raffiner l'approche et de l'adapter à d'autres contextes.

CHAPITRE 5 ÉLABORATION DE L'ISC

Ce chapitre est consacré à la conception de l'ISC, l'outil que nous proposons pour établir une connaissance et une compréhension commune de l'environnement technologique et de son utilisation, et ainsi améliorer la collaboration inter-équipe. Nous y détaillerons pourquoi les logiciels d'application constituent le point de départ stratégique pour cette ISC et nous explorerons également les trois dimensions clés qui nous permettront de bâtir une compréhension holistique de l'environnement technologique et de son utilisation. Pour finir, ce chapitre présentera la démarche pour initier une approche collaborative pertinente et adaptée aux réalités complexes des organisations, par le biais de la création et la validation d'une l'ISC.

5.1 Bases de l'ISC dans un contexte de technologies numériques

Comme exploré à la section 2.1, le terme « technologies numériques » englobe l'infrastructure informatique, les logiciels système, les logiciels d'application et les appareils utilisateurs. Ces quatre groupes de technologies sont profondément interdépendants : les appareils utilisateurs permettent d'interagir avec les logiciels d'application, les logiciels d'application sont à leur tour supportés par des logiciels système, qui sont eux-mêmes supportés par l'infrastructure informatique.

Cependant, les logiciels de système et l'infrastructure informatique sont généralement connus et visibles uniquement par l'équipe TI ; seuls les logiciels d'application et les appareils utilisateurs sont connus de tous. C'est en partie pourquoi la présente étude se concentre principalement sur les logiciels d'application de l'organisation comme base pour l'ISC. Ces derniers représentent le point de contact direct entre l'utilisateur et la technologie, offrant ainsi l'avantage d'être familiers à tous les intervenants impliqués dans la création et la mise à jour des stratégies de continuité des activités :

- Les gestionnaires en sont les principaux utilisateurs.
- L'équipe de continuité les recense dans le cadre du PCA.
- L'équipe TI les intègre au PRI (à moins qu'ils ne fassent partie du *Shadow IT*, un point sur lequel nous reviendrons à la section 5.1.3).

Au-delà de leur position stratégique et de leur familiarité, l'étude des logiciels d'application permet aux intervenants d'établir des points de référence communs qui symbolisent la complexité

inhérente aux environnements technologiques et opérationnels. En d'autres termes, les logiciels d'application, par l'entremise de l'ISC, deviennent un point de discussion concret à travers lequel les intervenants peuvent améliorer leur connaissance des technologies numériques et de leur utilisation et établir une compréhension commune de la complexité globale de l'environnement technologique. Du côté technique, bien que les logiciels d'application puissent paraître simples aux yeux de l'utilisateur, ils reposent sur des systèmes sous-jacents complexes et interdépendants. Pour ajouter à cette complexité, les logiciels d'application peuvent également entretenir des liens de dépendance entre eux par l'intermédiaire d'un intergiciel, que nous considérons comme un logiciel de système, comme expliqué à la section 2.1.2. Prenons l'exemple d'un logiciel d'application de gestion de tâches comme Asana, qui peut être connecté à un outil de messagerie instantanée comme Teams : lorsqu'une tâche est assignée ou mise à jour dans Asana, une notification automatique peut être envoyée dans un canal spécifique de Teams. Ce niveau élevé d'interdépendance, bien qu'il puisse augmenter la productivité, signifie qu'une perturbation à n'importe quel niveau — de l'infrastructure informatique aux logiciels système, allant jusqu'à d'autres logiciels d'application — peut avoir des impacts directs sur un ou plusieurs logiciels d'application, puisque ces derniers se trouvent au dernier niveau de l'arborescence technologique (*technology stack* en anglais). De plus, comme exploré au chapitre 2, l'externalisation de certaines technologies numériques peut complexifier davantage cet environnement en partageant les responsabilités de maintien, de mise à jour et de support entre plusieurs équipes, internes ou externes. Du côté opérationnel, les logiciels d'application sont omniprésents et intrinsèques aux opérations quotidiennes de l'organisation. En effet, comme mentionné au chapitre 3, ils sont utilisés à diverses fins, et l'importance des fonctionnalités d'un logiciel d'application peut varier, ajoutant une couche de complexité opérationnelle à leur gestion et à leur intégration au PCA.

Les logiciels d'application se situent donc, par leur nature transversale, à l'intersection de la technologie et des opérations et de ce fait, à l'intersection du PCA et du PRI. La figure 5.1 ci-après illustre visuellement cette position centrale au sein de l'organisation. Elle met en évidence les logiciels d'application (en rouge), qui sont soutenus par les logiciels de système (en bleu) et qui sont directement au service des opérations (en jaune). Bien que cette figure ne représente pas une organisation spécifique, elle sert à démontrer la complexité d'un environnement technologique moderne. On y observe que chaque composante des quatre niveaux de technologies numériques peut être détenue et contrôlée en interne ou par des entités externes. De plus, un logiciel

d’application ou de système interne peut être pris en charge par une infrastructure externe, et inversement, un logiciel de système externe peut soutenir un logiciel d’application interne. La figure illustre également qu’un même logiciel d’application peut être supporté par plusieurs logiciels de système. De même, l’infrastructure informatique – représentée ici par des serveurs (en turquoise) – peut supporter une multitude de logiciels de système. Bien que ce niveau de l’infrastructure informatique comprenne divers composants, la figure 5.1 se concentre sur les serveurs pour illustrer cette capacité de support multiple.

À droite de la figure, les domaines d’application du PCA et le PRI sont représentés. C’est la zone de chevauchement (en vert) entre ces deux plans, couvrant les appareils utilisateurs et les logiciels d’application, qui constitue leur point d’intersection crucial. En effet, on y voit clairement que les activités et processus considérées dans le PCA dépendent intrinsèquement de la disponibilité des logiciels d’application, qui elle-même dépend des logiciels et de l’infrastructure informatique qui font l’objet du PRI. C’est donc dans cette zone d’intersection, plus précisément la portion liée aux logiciels d’application, que la proposition d’ISC de cette étude s’inscrit.

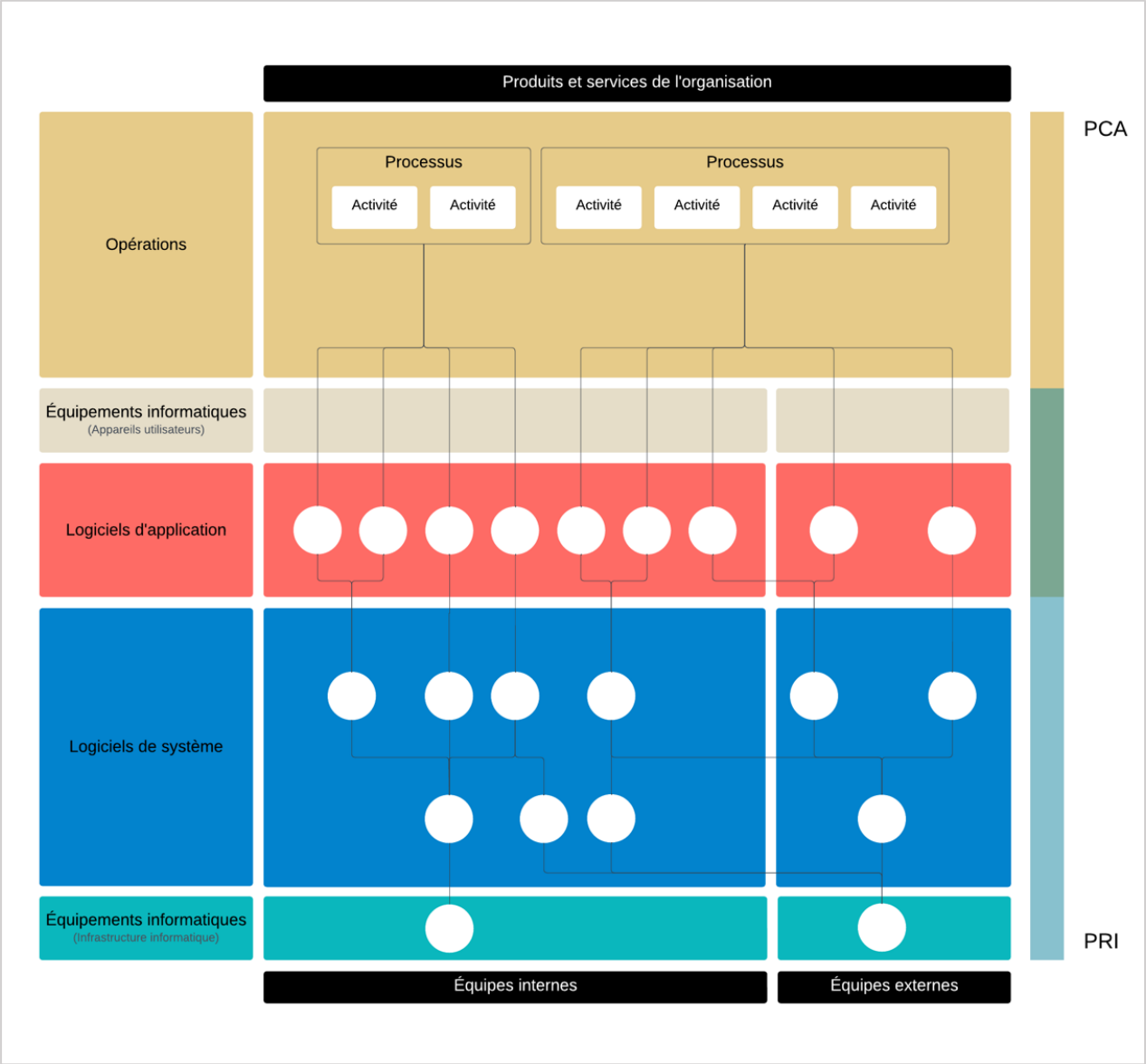

Figure 5.1 Positionnement des logiciels d'application dans l'organisation

5.2 Dimensions de l'ISC

Afin de développer une connaissance et une compréhension holistique des logiciels d'application, nous avons choisi de considérer ces derniers, en tant que groupe, sous trois dimensions clés qui seront explorées en détail dans cette section : le type d'utilisation, les modalités d'utilisation et la portée d'utilisation. A priori, nous avons sélectionné ces dimensions parce qu'elles permettent de répondre à des questions à la fois élémentaires et fondamentales sur l'utilisation des logiciels d'application : *pour faire quoi ? comment ? par qui ?* Ces dimensions serviront par la suite de base pour orienter et structurer l'ISC. Afin de nous assurer qu'elles étaient claires et pertinentes, les

dimensions ont été validées par des intervenants du domaine de la continuité des activités dans le cadre d'un atelier, ce dernier sera expliqué en détail à la section 5.2.4. Les prochaines sections exploreront le détail de ces trois dimensions, le raisonnement derrière ces choix et les résultats de la validation.

5.2.1 Type d'utilisation

Nous nous intéresserons tout d'abord aux différentes façons dont les logiciels d'application peuvent être utilisés. Devant le grand nombre de logiciels d'application disponibles sur le marché, nous avons choisi de concentrer nos efforts sur les logiciels de bureautique de type SaaS pour leur utilisation répandue, leur accessibilité en ligne et leurs fonctionalités axées sur le travail en équipe. Bien qu'il n'existe pas de consensus sur le pourcentage d'organisations qui utilisent des logiciels de bureautique de type SaaS, au Québec, en 2023, c'était 89,9 % des organisations de plus de 250 employés et de 75,8 % des organisations de 50 à 249 employés qui utilisaient ce type de logiciels pour collaborer ou communiquer (Gouvernement du Québec, 2024).

Afin de mieux comprendre et détailler l'utilisation de ce type de logiciels de bureautique dans l'organisation, nous les avons décomposé en trois catégories spécifiques : soit les logiciels de communication, d'organisation et de collaboration, qui seront détaillés dans les sous-sections à venir. Ces catégories d'utilisation, qui offrent une bonne couverture des fonctionnalités qui permettent aux équipes de rester connectés, offrent des angles concrets pour explorer le travail en équipe, structurer l'ISC et ultimement, entamer une réflexion collective sur les activités et les processus qui pourraient être affectés lors d'une perturbation.

5.2.1.1 Outils de communication

Nous définissons les outils de communication comme les logiciels de bureautique utilisés pour faciliter le dialogue et l'échange d'informations de façon instantanée ou dans un délai très court, entre individus ou groupes. En général, les informations échangées sont en format texte, voix ou vidéo. Voici quelques exemples d'outils de communication populaires dans les organisations (Hoory, 2023) :

- Courriel : Outlook, Gmail
- Messagerie instantanée : Teams, Slack, Google Chat, iMessage
- Voix et vidéo : Zoom, Teams, Webex, Google Meet

Il est à noter que la croissance du télétravail, entre autre due à la pandémie de COVID-19, a entraîné une augmentation significative de l'utilisation des outils de communication (Paerata, 2023). En général, cette catégorie d'outils requiert un niveau de connectivité et de performance élevé puisque l'échange d'information doit prendre place dans un court laps de temps pour rencontrer les exigences au niveau de la productivité et de l'expérience utilisateur.

5.2.1.2 Outils d'organisation

Nous définissons les outils d'organisation comme des logiciels de gestion, de coordination ou de planification des activités, des processus ou des ressources. Ce sont des outils qui peuvent être utilisés pour détailler, assigner et suivre l'avancement de tâches et d'objectifs. Ce sont également des outils qui peuvent être utilisés pour gérer l'assignation de ressources telles que des équipements ou de la main-d'œuvre. Considérant la vue d'ensemble que ces outils peuvent offrir aux gestionnaires, ils sont aussi fréquemment utilisés dans le processus de prise de décision. Voici quelques exemples d'outils d'organisation populaires :

- Outils de gestion de tâches : Asana, Monday.com, Trello, ClickUp, Wrike, Jira
- Outils de gestion des processus : Microsoft Power Automate
- Outils de gestion des ressources : SAP, Microsoft Dynamics 365, Float, Kantata, Saviom

Bien que les outils de type ERP soient considérés comme des outils d'organisation, nous ferons l'effort de les différencier et de les isoler dans la création de l'ISC, étant donné leur rôle crucial dans les opérations et leur utilisation à l'échelle de l'organisation. En effet, le logiciel ERP centralise et gère l'ensemble des activités d'une organisation, de la comptabilité à la production, en passant par la chaîne d'approvisionnement (Oracle, s. d.). Par conséquent, les informations sur sa portée d'application seront traitées séparément dans le contexte de l'ISC. Tout comme les outils de communication, les exigences de connectivité pour les outils d'organisation sont élevées puisque la coordination des tâches nécessite une compréhension de l'avancement et des bloqueurs en temps réel.

5.2.1.3 Outils de collaboration

Nous définissons les outils de collaboration comme des outils permettant le partage, la consultation ou la modification simultanée de fichiers par plusieurs utilisateurs. Il peut, par exemple, s'agir d'un espace de travail partagé avec accès à des fichiers, permettant aux utilisateurs de collaborer en

fonction de leurs permissions et de suivre l'historique des modifications. On pense, par exemple, à des outils comme Google Workspace (Drive, Docs, Sheets, Slides) ou Microsoft 365 (OneDrive, Word, Excel, PowerPoint).

En général, ces outils peuvent demeurer opérationnels, avec des fonctionnalités limitées, sans accès à internet. En ce sens, les exigences de connectivité peuvent être moins élevées. Cependant, tout comme les outils de communication et d'organisation, la portion interactive de l'outil requiert un niveau de connectivité élevé.

5.2.2 Modalités d'utilisation

Le deuxième angle sous lequel les logiciels de bureautique de type SaaS seront considérés est la façon dont les utilisateurs y accèdent. Bien qu'il existe plusieurs façons d'analyser cette dimension, nous avons choisi la notion de télétravail pour cette première version de l'ISC puisque le travail à distance a pris une envergure considérable pendant et après la pandémie de COVID-19. Même s'il y a eu un retour significatif au travail en présentiel au cours des deux dernières années, le télétravail et le mode de travail hybride persistent, représentant respectivement 26 % et 11 % de la main d'œuvre totale dans le dernier trimestre de 2024 (*Canadian Remote Work Statistics and Trends 2025*, 2025). Un sondage du BCI auprès d'organisations ayant déjà mis en place une démarche de continuité révèle que plus de 30 % de leur personnel s'attend à pouvoir travailler à distance une partie du temps. Bien que 66,8 % des organisations répondantes aient déclaré que les mêmes normes de continuité s'appliquent aux travailleurs à distance/hybrides et en présentiel, une minorité notable n'a pas encore abordé cette question (The Business Continuity Institute, 2023).

Lorsqu'une organisation permet le télétravail, elle peut avoir mis une politique de télétravail en place. Généralement, la politique de télétravail décrira un ensemble de règles pour encadrer le travail effectué par ses employés à l'extérieur des locaux de l'organisation. Cette politique peut, entre autres, contenir la fréquence et les plages horaires autorisées, des informations sur les appareils utilisateurs autorisés et des mesures à respecter pour protéger les informations de l'organisation, par exemple la connexion à un réseau privé sécurisé, tel qu'un VPN, qui peut introduire son lot de complexités techniques. En effet, comme détaillé au chapitre 2, ce type de réseau offre une porte d'entrée unique vers d'autres logiciels d'application. En cas de panne ou de défaillance, c'est donc l'ensemble de la main-d'œuvre en télétravail qui peut se retrouver simultanément sans accès à plusieurs logiciels. La pertinence de cette dimension pour l'ISC réside

donc dans la nouveauté et l'ampleur du phénomène, ainsi que dans les défis technologiques qu'il présente pour l'accès aux logiciels d'application.

5.2.3 Portée d'utilisation

La portée d'utilisation vise à définir par qui et pour travailler avec qui les logiciels de bureautique de type SaaS sont utilisés. Cette catégorie vise à mieux comprendre la portion des logiciels sujette à une utilisation participative, qu'elle soit interne ou externe. Par exemple, un logiciel peut être limité à un usage interne, au sein d'une même équipe ou entre différentes équipes de l'organisation. Inversement, le logiciel peut également faciliter le travail avec des entités externes telles que des fournisseurs, des clients ou des partenaires. Ce cas de figure est non négligeable puisque les projets multi-équipes et multi-organisations en mode virtuel sont de plus en plus fréquents (Ledwith & Ludden, 2016).

Cette dimension nous permettra également d'identifier les disparités entre l'utilisation rapportée par les gestionnaires et l'utilisation recensée par l'équipe TI. Cela nous permettra donc de potentiellement déceler l'utilisation de logiciels de logiciels de bureautique de type SaaS qui pourraient ne pas avoir été autorisés par l'équipe TI, ouvrant ainsi la voie à des investigations supplémentaires et ultimement, à la réduction du phénomène *Shadow IT*.

5.2.4 Validation des dimensions

Afin de valider la clarté et la pertinence des dimensions sélectionnées pour l'ISC – à savoir le type d'utilisation, les modalités d'utilisation et la portée d'utilisation – nous avons organisé un atelier de validation. Cet atelier, qui rassemblait environ 60 professionnels de la continuité des activités, avait pour objectif de recueillir les retours de professionnels expérimentés et de s'assurer que ces dimensions étaient non seulement claires, mais aussi appropriées pour l'élaboration d'une ISC pertinente. Il s'agissait d'une étape cruciale pour confirmer que notre cadre d'analyse correspondait aux réalités et aux besoins des différents intervenants en matière de continuité des activités. Cette section détaille les observations et les conclusions tirées de cette validation pour chaque dimension.

Du côté de la dimension « type d'utilisation », nous avons constaté une bonne compréhension générale de nos trois sous-catégories, mais avec une nuance importante : si la catégorie des outils de communication s'applique à la majorité des organisations, ce n'est pas nécessairement le cas pour les outils d'organisation et de collaboration. Certaines organisations utilisent en effet peu ou

pas de logiciels dédiés à l'organisation ou à la collaboration, privilégiant des méthodes manuelles telles que des tableaux blancs, des calendriers papier, une circulation manuelle de documents et des rencontres en personne. Les outils de communication, quant à eux, se sont non seulement révélés bien compris de tous, mais ils ont aussi suscité des discussions animées et sont ressortis comme une catégorie de logiciels essentielle dans les opérations de plusieurs organisations. L'atelier nous a également permis d'observer des discussions sur les mesures de repli à mettre en œuvre à la suite d'une perturbation. Au cours de ces échanges, il est devenu évident que plusieurs organisations n'avaient pas abordé les logiciels de bureautique de type SaaS, plus précisément nos trois catégories d'utilisation, dans leurs PCA, et que les membres d'une même équipe n'avaient pas systématiquement une vision uniforme de la perturbation et de ses impacts potentiels sur les activités. En effet, certains participants nous ont mentionné que les logiciels de bureautique de type SaaS n'avaient pas été considérés durant l'élaboration et la mise à jour de stratégies de continuité des activités, leur utilisation étant parfois perçue comme secondaire aux activités critiques.

En général, la majorité des organisations ont indiqué que l'indisponibilité des logiciels de bureautique de type SaaS entraînerait des impacts significatifs à court terme, les outils de communication demeurant les plus problématiques. Ces observations nous ont donc permis de confirmer la pertinence d'utiliser ce type de logiciels pour cette étude, et particulièrement les types d'utilisation sélectionnés, comme base structurelle pour la création de l'ISC.

Du côté de la dimension relative à la portée d'utilisation des logiciels de bureautique de type SaaS, alors que plusieurs intervenants avaient déjà pris en compte les tâches et interactions réalisées en interne via certains logiciels, nous avons constaté que l'aspect externe semblait négligé. Les discussions générées par cette notion ont confirmé la pertinence de cette dimension. L'atelier ne nous a malheureusement pas permis de valider la pertinence du sujet *Shadow IT* puisque son format n'a pas permis de comparer les réponses de gestionnaires avec celles de l'équipe TI pour une même organisation. En raison du temps limité de l'atelier, il n'a pas non plus été possible de valider la dimension « modalités d'utilisation ».

Bien que l'atelier ait confirmé la pertinence de plusieurs dimensions sélectionnées, la diversité des réponses et des échanges a aussi démontré que les dimensions devaient être adaptées à chaque organisation. En d'autres termes, l'ISC doit être caractérisée pour chaque organisation. Pour ce faire, il est important d'obtenir certaines informations sur l'organisation avant de procéder à la

collecte d'information qui seront nécessaire pour créer l'ISC, nous explorerons ce point en détail à la section suivante.

5.3 Proposition d'une démarche pour initier une approche collaborative

Comme constaté au chapitre 3, dans plusieurs organisations, les gestionnaires, l'équipe de continuité et l'équipe TI peinent à établir une connaissance et une compréhension commune de leur environnement technologique et de son utilisation. Cette situation peut mener à une collaboration difficile entre les équipes et des lacunes au niveau des activités entourant la préparation aux perturbations, notamment dans la création et la mise à jour de stratégies de continuité des activités. Le concept d'unité d'effort qui a été exploré à la section 4.1, supporté par la création et la validation d'une ISC, peut contribuer à atténuer ces lacunes. Comme détaillé à la section 4.1, l'ISC est élaborée à partir d'informations et de jugement professionnels provenant de diverses sources, lesquelles sont ensuite mises en commun, synthétisées, visualisées et présentées de façon à être facilement comprises par tous les intervenants. La validation de l'ISC par les intervenants et les discussions qui en découlent peuvent améliorer significativement la connaissance et la compréhension commune de l'environnement technologique et de son utilisation et ultimement, peuvent permettre de renforcer la collaboration inter-équipes.

C'est dans cette optique que nous proposons une démarche structurée pour créer et valider une ISC. Cette démarche, qui implique les gestionnaires, l'équipe de continuité et l'équipe TI, s'articule autour de la création d'une ISC qui sera alimentée par les informations collectées au sein de l'organisation, en prenant en considération les dimensions explorées à la section 5.2. L'ISC sera ensuite validée avec les intervenants clés, ouvrant ainsi la voie à l'harmonisation dans les stratégies de continuité des activités. La présente section a pour objectif d'expliquer cette démarche collaborative, en détaillant ses six étapes clés.

5.3.1 Étape 1 : former l'équipe et comprendre les besoins

La première étape de la démarche consiste à créer une équipe de travail qui pilotera la démarche. L'équipe devrait idéalement être composée de représentants des deux sphères clés appelées à collaborer dans le cadre de cette démarche : un expert du domaine technologique et un expert de l'équipe de continuité. Plus concrètement, cette équipe devrait donc comprendre un représentant

de l'équipe TI et un représentant de l'équipe de continuité. Pour éviter la confusion, nous nommerons l'équipe de travail ainsi formée « équipe ISC ».

Dans un premier temps, l'équipe ISC aura pour mission d'identifier les gestionnaires qui fourniront les données essentielles à la création de l'ISC et qui participeront à sa validation. Puisque l'ISC vise à fournir des informations sur l'utilisation des logiciels de bureautique de type SaaS à l'échelle de l'organisation, il sera nécessaire d'identifier des gestionnaires de toutes les équipes de l'organisation afin d'obtenir une couverture complète.

À cette étape, nous recommandons d'organiser une rencontre préliminaire avec les membres de l'équipe ISC. L'objectif principal de cette rencontre est de passer en revue les étapes de la démarche afin de gérer les attentes de l'équipe. Les membres de l'équipe ISC pourront ensuite identifier les défis et les besoins clés liées à la compréhension de l'environnement technologique et de son utilisation. Cette discussion donnera le coup d'envoi aux étapes 2 et 3 qui seront explorées dans les prochaines sections, et sera essentielle pour établir une ISC qui répond aux besoins de l'organisation.

Il est à noter qu'à cette étape, ainsi qu'aux étapes subséquentes, l'équipe ISC pourra potentiellement découvrir de nouvelles pistes à explorer ou être tentée d'élargir le périmètre de la démarche, risquant ainsi de passer prématurément en mode de résolution de problèmes. Nous conseillons de rester rigoureusement focalisé sur les étapes de la démarche, afin d'assurer l'atteinte des objectifs fixés.

5.3.2 Étape 2 : caractérisation de l'ISC

Il est crucial que l'ISC soit structurée pour répondre aux besoins spécifiques et à l'environnement technologique de l'organisation. Dans cette optique, nous recommandons que l'équipe ISC réponde d'abord à quelques questions préliminaires. Cet exercice permettra d'affiner les dimensions de l'ISC (type d'utilisation, modalités d'utilisation et portée d'utilisation) et d'orienter la collecte d'informations subséquente, que nous explorerons à la prochaine section. Ces questions devront être adaptées au contexte spécifique de l'organisation.

Pour illustrer l'apport des questions préliminaires sur l'affinage des dimensions et la caractérisation de l'ISC, nous présentons ci-dessous quelques exemples, détaillant comment chaque question aide à préciser une dimension particulière.

- L'organisation utilise-t-elle des logiciels d'organisation et de collaboration ?
    - Cette question, liée à la dimension « type d'utilisation », permet de déterminer si tous les types d'utilisation de logiciels de bureautique de type SaaS (communication, organisation et collaboration) sont pertinents pour l'organisation à l'étude. En effet, bien que les logiciels de communication soient pertinents pour la grande majorité des organisations, les logiciels d'organisation et de collaboration, quant à eux, ne sont pas nécessairement utilisés, il est donc important de confirmer leur pertinence pour l'ISC.
- L'organisation utilise-t-elle un logiciel ERP ? Si oui, lequel ?
    - Également rattachée à la dimension « type d'utilisation », cette question peut être fondamentale car les logiciels ERP ne sont pas utilisés dans toutes les organisations. Si aucun logiciel ERP n'est utilisé, cette notion pourra être omise de l'ISC. Inversement, si l'organisation utilise un logiciel ERP, en connaître le nom et la façon dont il est utilisé dans l'organisation facilitera la collecte d'informations en permettant d'éviter les questions trop génériques. Ces détails seront également précieux lors de la validation de l'ISC, pour mieux orienter les discussions.
- L'organisation a-t-elle une politique de télétravail formelle ?
    - Cette question relève de la dimension « modalités d'utilisation ». Il peut être pertinent de savoir si le télétravail est autorisé et encadré avant d'amorcer la collecte d'informations. Si le télétravail n'est pas permis, cette dimension pourra être omise de l'ISC. Si une politique de télétravail existe, l'exploration de cette dimension durant la collecte d'informations pourra se faire sous un angle différent, par exemple en se concentrant sur son application spécifique ou ses défis. Si la politique est inexistante ou peu précise, cela pourrait indiquer une zone à approfondir dans l'ISC.
- L'organisation dispose-t-elle d'un processus officiel d'approbation pour les logiciels d'application utilisés ?
    - Cette question, qui se rapporte à la dimension « portée d'utilisation », offre un aperçu du niveau de contrôle de l'équipe TI sur l'environnement technologique de l'organisation. Si l'organisation ne possède pas de processus formel d'approbation des logiciels ou ne restreint pas leur installation, cela peut indiquer une présence potentielle de *Shadow IT*. Dans un tel scénario, le rôle de cette question préliminaire

est de signaler l'importance de sonder attentivement l'étendue des logiciels non officiellement reconnus durant l'étape de collecte d'informations afin de mettre en lumière les disparités potentielles dans l'ISC.

Il est important de souligner que cette liste de questions n'est pas exhaustive et que, lors de l'application de la démarche au sein d'une organisation, ces questions devront être adaptées à son contexte et à son environnement technologique. L'objectif de ces questions demeure de mieux structurer l'ISC en identifiant les informations les plus pertinentes.

5.3.3 Étape 3 : collecte d'informations

L'ISC doit être fondée sur deux piliers : des informations concernant l'utilisation des logiciels de bureautique de type SaaS et des informations techniques et opérationnelles sur l'environnement technologique. Cette dualité est essentielle pour aligner la vision opérationnelle, détenue par les gestionnaires, et la vision technique, détenue par l'équipe TI, et ainsi renforcer la compréhension commune de l'environnement technologique et de son utilisation.

Du côté des informations d'utilisation relatives aux logiciels de bureautique de type SaaS, l'objectif est d'obtenir une vue d'ensemble, en se basant sur nos trois dimensions, soit le type d'utilisation, les modalités d'utilisation et la portée d'utilisation, ainsi que sur les précisions obtenues à l'étape 2 de cette démarche. Bien que diverses méthodes de collecte d'informations soient envisageables — entretiens, observation, analyse documentaire —, nous recommandons le questionnaire en ligne. Ce dernier a l'avantage de pouvoir être simultanément partagé à un grand nombre de participants. Il est également facile à compléter, ce qui peut, par conséquent, augmenter le taux de participation. Le format en ligne offre également l'avantage de fournir des données sur le comportement des utilisateurs, ce qui peut aider à identifier des points d'amélioration potentiels au niveau des questions. Par exemple, un temps de réponse élevé à une question peut indiquer que la question n'est pas suffisamment claire. Le questionnaire doit rester concis, idéalement complété en moins de 5 minutes. L'objectif n'est pas de forcer le répondant à détailler son utilisation avec une grande précision, mais plutôt de fournir des informations à la fois sommaires mais suffisament ciblées pour alimenter l'ISC. Les questions doivent être simples, et idéalement binaires ou à choix de réponses multiples, afin de faciliter la consolidation des informations qui devra être effectuée lors de la création de l'ISC. Suivant la suggestion de Charmont (2025), nous recommandons d'intégrer des options de réponse telles que « inconnu » ou « je ne sais pas ». Ces choix ne sont pas de simples

échappatoires ; ils agissent comme des indicateurs diagnostiques précieux pour l'ISC. Ils peuvent en effet révéler des enjeux sous-jacents, comme un manque de connaissance chez les répondants, un désengagement vis-à-vis du sujet, ou même une formulation ambiguë des questions.

Bien que la structure du questionnaire doive être adaptée au contexte de l'organisation, nous recommandons de centrer sa conception autour de la dimension « type d'utilisation ». Par exemple, une section pourrait être dédiée à chaque type d'utilisation jugé pertinent pour l'organisation, tel que déterminé à l'étape 2 de la démarche. Les dimensions « modalités d'utilisation » et « portée d'utilisation » peuvent ensuite être intégrées sous forme de sous-questions au sein de chaque section, toujours en s'appuyant sur les précisions obtenues lors de l'étape 2. Cette priorité donnée aux types d'utilisation se justifie par sa capacité à stimuler la réflexion des répondants sur leurs activités et sur les conséquences opérationnelles potentielles, pour l'ensemble de l'organisation, en cas de perturbation. En effet, en mettant l'emphase sur la communication, l'organisation et la collaboration, les gestionnaires peuvent mieux analyser l'utilisation des logiciels en contexte du travail intra et inter équipe. Afin d'illustrer cette structure, un exemple de questionnaire est présenté à l'annexe A.

En parallèle à cette collecte d'informations sur l'utilisation des logiciels de bureautique de type SaaS et dans le but de compléter l'ISC, il est crucial d'obtenir des données plus précises concernant l'environnement technologique. Puisqu'elle porte sur des détails techniques, cette portion de la collecte d'information doit s'effectuer auprès de l'équipe TI. Considérant que cette équipe gère l'ensemble des technologies numériques, la collecte d'informations peut être effectuée auprès d'un seul intervenant de l'équipe. Ces informations peuvent être recueillies à l'aide d'un questionnaire adapté au domaine de compétence et au vocabulaire de cette équipe ; nous en présentons un exemple générique à l'annexe B. Cependant, lorsque le temps et les ressources de l'équipe le permettent, nous recommandons plutôt l'entretien individuel. L'entretien offre plusieurs avantages : il permet de poser des questions plus pointues et de demander des clarifications, garantissant ainsi une compréhension plus nuancée des informations techniques. Il offre également l'opportunité de mieux comprendre les dynamiques et les rapports que l'équipe TI entretient avec le reste de l'organisation. Ces informations peuvent contribuer à orienter les discussions lors de l'atelier de validation de l'ISC, tout en révélant des nuances sur les interdépendances technologiques, les pratiques non documentées, ou les contraintes techniques qui sont plus difficiles à déceler sur papier.

La collecte d'informations, tant auprès des gestionnaires que de l'équipe TI, doit trouver un juste équilibre. Les données doivent avoir un niveau de détail suffisant pour que l'ISC produite soit pertinente et suscite des discussions constructives. Il est cependant crucial d'éviter un niveau de détail excessif, car cela pourrait alourdir le processus pour les participants et générer des discussions trop précises ou isolées, ce qui nuirait à l'obtention de la perspective globale recherchée dans cette démarche.

5.3.4 Étape 4 : création de l'ISC

Une fois les informations recueillies auprès des gestionnaires et de l'équipe TI, elles doivent être mises en commun et synthétisées dans un format visuel et compréhensible pour tous, tel qu'un ou plusieurs tableaux ou graphiques. À cette étape, l'équipe est chargée de créer une ISC qui reflète les besoins clés identifiés lors de l'étape 1, tout en exploitant au mieux les données collectées à l'étape 3. Pour ce faire, elle doit analyser les variations entre les informations rapportées sur le type, les modalités et la portée d'utilisation des logiciels de bureautique de type SaaS et les informations techniques fournies par l'équipe TI. Cette analyse des variations est cruciale, car elle peut révéler un manque de compréhension ou d'alignement quant à l'environnement technologique et son utilisation, offrant ainsi des pistes précieuses pour structurer et présenter l'ISC. Bien que la nature des variations dépende des données collectées, nous présentons ici quelques exemples fictifs afin d'illustrer le type de variations qui peut être pertinent à explorer :

- Une ou plusieurs équipes rapportent utiliser un nombre d'outils de communication, d'organisation ou de collaboration supérieur à ce que l'équipe TI a autorisé.
- Le temps de travail à distance rapporté par les gestionnaires est considérablement différent de celui estimé par l'équipe TI.
- Les logiciels perçus comme inaccessibles à l'extérieur du VPN par les équipes ne représentent pas la configuration du VPN effectué par l'équipe TI.
- Les logiciels les plus utilisés en télétravail ne correspondent pas aux données obtenues par l'équipe TI.
- L'utilisation réelle d'un logiciel important est largement supérieure ou inférieure à l'estimé de l'équipe TI ou de l'équipe de continuité.

Suite à cette analyse, une ou plusieurs représentations visuelles doivent être conçues pour créer une ISC qui représente ces variations et qui, lorsque possible, fait un lien avec les besoin identifiés à

l'étape 1. Les variations qui auront été observées dans les données collectées doivent être illustrées dans l'ISC, de façon simple et compréhensible pour tous, sans perdre les nuances importantes ni introduire de surcharge visuelle. Nous recommandons également d'intégrer la notion de types d'utilisation dans l'ISC, selon les catégories pertinentes pour l'organisation. Cela permet de poursuivre la réflexion amorcée lors de la collecte de données sur la façon dont les logiciels de bureautique SaaS soutiennent le travail d'équipe. Au final, le choix du format de l'ISC dépendra de l'organisation ainsi que des données recueillies ; l'ISC doit permettre aux intervenants qui participeront à sa validation d'identifier eux-mêmes les problématiques communes qui en ressortent. Comme le rappelle Charmont (2025), l'ISC ne doit pas être une interprétation des informations obtenues à l'étape 3 ; elle doit plutôt présenter les données brutes afin que les parties prenantes puissent établir elles-mêmes leur propre interprétation des résultats.

Il est important que les intervenants de l'équipe ISC travaillent ensemble pour concevoir l'ISC puisque c'est au fil des échanges, des réflexions et des efforts d'analyse requis pour la concevoir que la compréhension commune de l'environnement technologique et de son utilisation se forge et s'améliore.

5.3.5 Étape 5 : validation de l'ISC

L'ISC prend sa pleine valeur lorsqu'elle est partagée et validée par les gestionnaires ayant été identifiés par l'équipe ISC à l'étape 1 et ayant participés à la collecte d'information. Cette validation s'opère idéalement par l'entremise d'un atelier collaboratif, offrant un cadre structuré aux intervenants pour :

- Valider la justesse de l'ISC : l'atelier permet aux participants de confirmer que l'ISC reflète la réalité organisationnelle et l'utilisation réelle des logiciels de bureautique de type SaaS.
- Faciliter les échanges : grâce au format visuel et accessible de l'ISC, l'atelier stimule des discussions ouvertes et constructives entre les intervenants.
- Identifier des problèmes : les participants peuvent y discuter des problématiques soulevées par l'ISC, réconcilier les informations divergentes et, par conséquent, améliorer la connaissance et la compréhension commune de l'environnement technologique et de son utilisation.

En somme, l'atelier marque la transition entre un constat de manque d'alignement des équipes vers une vision commune de l'utilisation des logiciels de bureautique de type SaaS et de leur

environnement technologique, transformant ainsi une vision fragmentée en une compréhension commune.

5.3.6 Étape 6 : application des constats issus de la validation de l'ISC

Pour donner suite aux échanges lors de la validation de l'ISC, les équipes de continuité et TI devront traduire ces informations en actions concrètes. L'objectif est, entre autres, de retravailler et d'harmoniser les stratégies de continuité. Bien que les ajustements différeront d'une organisation à l'autre, voici quelques exemples concrets pour illustrer ces retombées potentielles :

- Intégration de logiciels au PCA : si l'exercice de validation de l'ISC a révélé une utilisation intensive de certains logiciels non préalablement recensés dans le PCA, ces derniers pourront y être intégrés, des mesures de repli spécifiques pourront être développées et des valeurs ODR et RPO pourront ainsi leur être attribuées. Si leur utilisation avait été sous-estimée, l'équipe TI pourrait recalibrer l'attention et les ressources qui leur sont allouées dans le PRI.
- Gestion du *Shadow IT* : si l'exercice de validation a mis en lumière des logiciels utilisés au sein de l'organisation mais inconnus de l'équipe TI (phénomène de *Shadow IT*), ces logiciels pourront être officiellement recensés. Cela permettra d'intégrer des stratégies de gestion ou des mesures de repli pertinentes dans le PCA et le PRI. Des initiatives de sensibilisation pourraient également être mises en œuvre afin de rappeler quels sont les processus d'approbation des logiciels et d'informer sur les dangers liés à l'utilisation de logiciels non autorisés.
- Alignement des priorités et des mesures de repli : la compréhension partagée des priorités opérationnelles et des limites technologiques permettra d'harmoniser les mesures de repli entre le PCA et le PRI. Par exemple, si l'ISC révèle l'importance d'un logiciel non identifié auparavant, les équipes pourront collaborer pour concevoir des mesures de repli réalistes dans le contexte technologique de l'organisation, tout en répondant aux exigences opérationnelles.
- Amélioration de la connaissance des logiciels utilisés : l'ISC permettra de mieux appréhender l'utilisation réelle des logiciels, qu'ils aient été préalablement recensés ou non. Cette connaissance accrue offrira une meilleure compréhension de la vulnérabilité des opérations de l'organisation face à l'utilisation de certains types de logiciels, elle précisera

quelles fonctionnalités sont critiques et comment les activités seraient potentiellement affectées en cas de perturbation, aidant ainsi au choix et à la priorisation des mesures de repli.

Au-delà d'une meilleure harmonisation des plans, une compréhension mutuelle entre les deux équipes sera essentielle pour améliorer la communication, aligner les objectifs et faciliter la prise de décision, le tout se traduisant par une collaboration plus solide. Cela pourrait avoir des effets bénéfiques non seulement sur les stratégies de continuité des activités, mais aussi, plus globalement, sur la culture de l'organisation.

Il est important de noter que, compte tenu de la nature dynamique de l'environnement technologique et des évolutions organisationnelles, l'ISC n'est pas statique. Elle doit être régulièrement mise à jour pour conserver sa pertinence, et les révisions aux stratégies de continuité des activités doivent être appliqués de façon continue. La fréquence de ces mises à jour devrait être déterminée par l'équipe ISC, et le processus de révision doit également être encadré par celle-ci pour en assurer la cohérence et l'efficacité.

CHAPITRE 6 EXERCICE DE VALIDATION

Cette section détaille l'exercice de validation de la démarche que nous avons explicitée dans le chapitre 5. Nous y décrirons d'abord comment chaque étape de la démarche a été adaptée au contexte de l'organisation retenue pour cet exercice de validation. Ensuite, nous explorerons les constats concernant les bases et les dimensions de l'ISC ainsi que sur la démarche proposée, offrant ainsi un aperçu complet des apprentissages tirés de cet exercice concret. Finalement, nous suggérerons des pistes pour des futures itérations de la démarche, afin d'affiner cette dernière et de la rendre modulable.

6.1 Application de la démarche proposée

Cette section détaille les étapes clés de notre exercice de validation, mené en collaboration avec une municipalité d'environ 15 000 habitants, située en banlieue de Montréal. Nous y décrirons les étapes préliminaires incluant la définition des besoins et la collecte d'informations. Ensuite, nous présenterons l'étape de création de l'ISC, basée sur l'analyse des informations collectées. Enfin, la section explorera le déroulement de l'atelier de validation.

6.1.1 Préparation

Pour cet exercice de validation, l'équipe ISC était composée de notre équipe de recherche, du responsable de l'équipe TI de la municipalité et du responsable de l'équipe résilience, risques et catastrophes de la municipalité, ce dernier prenant le rôle de responsable de l'équipe de continuité dans le cadre de cet exercice. Nous avons amorcé l'exercice de validation par une première rencontre avec ces représentants de la municipalité. L'objectif principal était de bien comprendre le contexte technologique et opérationnel de la municipalité, ainsi que ses besoins spécifiques. Cette rencontre s'est avérée cruciale pour cerner les besoins suivants :

- Renforcement des stratégies de continuité : les représentants de la municipalité ont identifié un besoin de mieux définir les vulnérabilités opérationnelles liées à l'utilisation de logiciels de bureautique de type SaaS et de mettre en place des stratégies de continuité des activités, tant au niveau technologique qu'opérationnel, pour mieux soutenir les activités de la municipalité en cas de perturbation.

- Soutien à l'équipe TI : les représentants de la municipalité ont noté la disponibilité limitée de l'équipe TI et le besoin d'améliorer la compréhension commune de son rôle et du niveau de contrôle qu'elle peut exercer sur l'environnement technologique.

Cette rencontre préliminaire a non seulement permis d'éclaircir les besoins de la municipalité, mais aussi de recueillir les premières informations nécessaires pour caractériser la future ISC, marquant ainsi le début de l'étape 2 de notre démarche. Grâce à ces informations préliminaires, nous avons pu concevoir une première version d'un questionnaire en ligne. Celui-ci visait à collecter, auprès des gestionnaires de la municipalité, les informations nécessaires à la création de l'ISC, chaque gestionnaire étant invité à analyser les outils utilisés par son équipe pour y répondre. Le devancement de l'étape de création du questionnaire nous a permis de présenter notre démarche à l'équipe ISC de façon plus concrète lors d'une deuxième rencontre, jumelant ainsi les étapes 2 et 3 de la démarche proposée. Cette approche a stimulé une collaboration productive qui nous a permis d'affiner les questions conjointement avec les représentants de la municipalité, en demandant des précisions au besoin et en assurant ainsi une meilleure adéquation avec l'environnement technologique. Cette deuxième rencontre nous a donc permis de valider le questionnaire préliminaire mais aussi de recueillir certaines informations cruciales relativement aux trois dimensions explorées à la section 5.2 :

- Type d'utilisation : les représentants de la municipalité ont confirmé une utilisation limitée des logiciels de collaboration, les utilisateurs préférant souvent les outils de communication, comme Outlook ou Teams, à ces fins. Des questions à ce sujet ont tout de même été incluses au questionnaire afin de valider cette observation, bien que nous anticipions que ce type d'utilisation ne serait pas prépondérant dans l'ISC. La présence d'un logiciel ERP a également été confirmée, menant à l'inclusion de questions spécifiques à ce dernier au questionnaire.
- Modalités d'utilisation : les représentants de la municipalité ont indiqué que le télétravail est permis mais qu'aucune politique de télétravail n'a officiellement été diffusée. L'utilisation d'un VPN pour accéder à la majorité des logiciels à distance, sauf les outils de communication, a également été confirmée. Conformément à l'étape 2 de notre démarche, nous avons donc inclus des questions relativement à la proportion de télétravail ainsi que les connaissances des utilisateurs quant au VPN et à son utilisation, afin de pouvoir illustrer ces informations dans l'ISC.

- Portée d'utilisation : le responsable de l'équipe TI a confirmé que la municipalité dispose de dispositifs technologiques bloquant l'installation de logiciels non autorisés, signalant ainsi le désir de la municipalité d'exercer un contrôle sur son environnement technologique. Bien que ce type de dispositif puisse réduire le problème de *Shadow IT*, cela ne l'élimine pas complètement puisque des logiciels de type SaaS peuvent être utilisés sans nécessairement être téléchargés et installés par les utilisateurs. Nous avons ainsi intégré des questions sur le nombre d'outils utilisés, dans le but de potentiellement illustrer la présence de *Shadow IT* dans l'ISC.

Pour répondre au besoin de développer des stratégies de continuité des activités exprimé par les représentants de la municipalité dès la première rencontre, nous avons intégré des questions sur les délais d'impacts significatifs sur les opérations en cas d'indisponibilité de certains outils. L'objectif de ces questions était de mettre en lumière l'importance de ces logiciels et ainsi favoriser les échanges lors de l'atelier de validation. Quant au besoin de soutien à l'équipe TI également exprimé lors de la première rencontre, nous avons plutôt décidé d'aborder ce point durant l'atelier de validation de l'ISC afin de limiter la portée du questionnaire et de ne pas surcharger l'ISC.

Cette deuxième rencontre avec les intervenants de la municipalité nous a donc permis de compléter notre caractérisation de l'ISC et par le fait même, de finaliser le questionnaire servant de base à la collecte de données, complétant ainsi les étapes 2 et 3 de la démarche. Le questionnaire anonymisé peut être consulté à l'annexe C.

6.1.2 Création de l'ISC

Le questionnaire a été envoyé à 20 gestionnaires, choisis par le responsable de l'équipe résilience, risques et catastrophes de la municipalité. Comme précisé à la section précédente, chaque gestionnaire devait analyser l'utilisation des outils au sein de son équipe pour y répondre. Nous avons ensuite analysé et compilé les réponses des 11 questionnaires complétés qui nous ont été retournés, nous afin d'identifier les enjeux de compréhension et d'illustrer l'utilisation des logiciels de bureautique de type SaaS. Pour synthétiser ces informations, trois figures ont été préparées, complétant ainsi l'étape 4 de notre démarche.

Considérant l'intérêt généré par les outils de communication lors du premier atelier, les informations préliminaires dont nous disposions concernant l'environnement technologique de la municipalité et les variations enregistrées entre les données d'utilisation et l'information fournie

par l'équipe TI, nous avons dédié deux figures à ce type d'outil dans la création de l'ISC. La première figure, présentée ci-après, couvre les dimensions « type d'utilisation » et « portée d'utilisation ». Elle illustre le nombre total d'outils de communication utilisés par équipe, incluant les outils employés à l'interne ainsi que les outils additionnels utilisés pour communiquer à l'externe, soit avec des fournisseurs ou des partenaires, visant ainsi à faire réfléchir sur les types d'activités qui seraient affectées par une perturbation. Par exemple, le gestionnaire de l'équipe 1 a indiqué que son équipe utilise trois outils pour la communication à l'interne et un outil additionnel pour communiquer avec l'externe, totalisant ainsi quatre outils. Des barres pointillées représentent les gestionnaires d'équipe qui n'ont pas été en mesure de quantifier le nombre d'outils externes utilisés, signalant une possible zone d'ombre opérationnelle et technologique à explorer ; c'est par exemple le cas du gestionnaire de l'équipe 4, qui a indiqué que son équipe utilisait deux outils en interne mais ignorait l'usage d'outils additionnels pour l'externe. Quant à eux, les points violets indiquent les répondants ayant déclaré n'utiliser aucun outil de communication interne ou externe, soulevant une potentielle incompréhension de la question ou de l'environnement technologique. À titre d'exemple, les gestionnaires des équipes 9, 10 et 11 ont mentionné que leur équipe n'utilisait aucun outil pour communiquer à l'interne, celui de l'équipe 9 indiquant ne pas savoir si des outils étaient employés pour communiquer avec l'externe au sein de son équipe. Enfin, une ligne horizontale met en évidence le nombre de logiciels officiellement autorisés par l'équipe TI, soit deux logiciels, soulignant les dépassements et visant ainsi à stimuler les discussions autour du phénomène *Shadow IT* lors de la validation de l'ISC. Par exemple, les équipes 1, 2 et 3 utilisent un nombre d'outils supérieur au seuil autorisé par l'équipe TI. Les équipes 4 et 9 pourraient également potentiellement dépasser ce seuil d'outils autorisés, mais l'incertitude quant à l'utilisation d'outils externes par leurs gestionnaires, comme mentionné précédemment, nous empêche de confirmer ces informations.

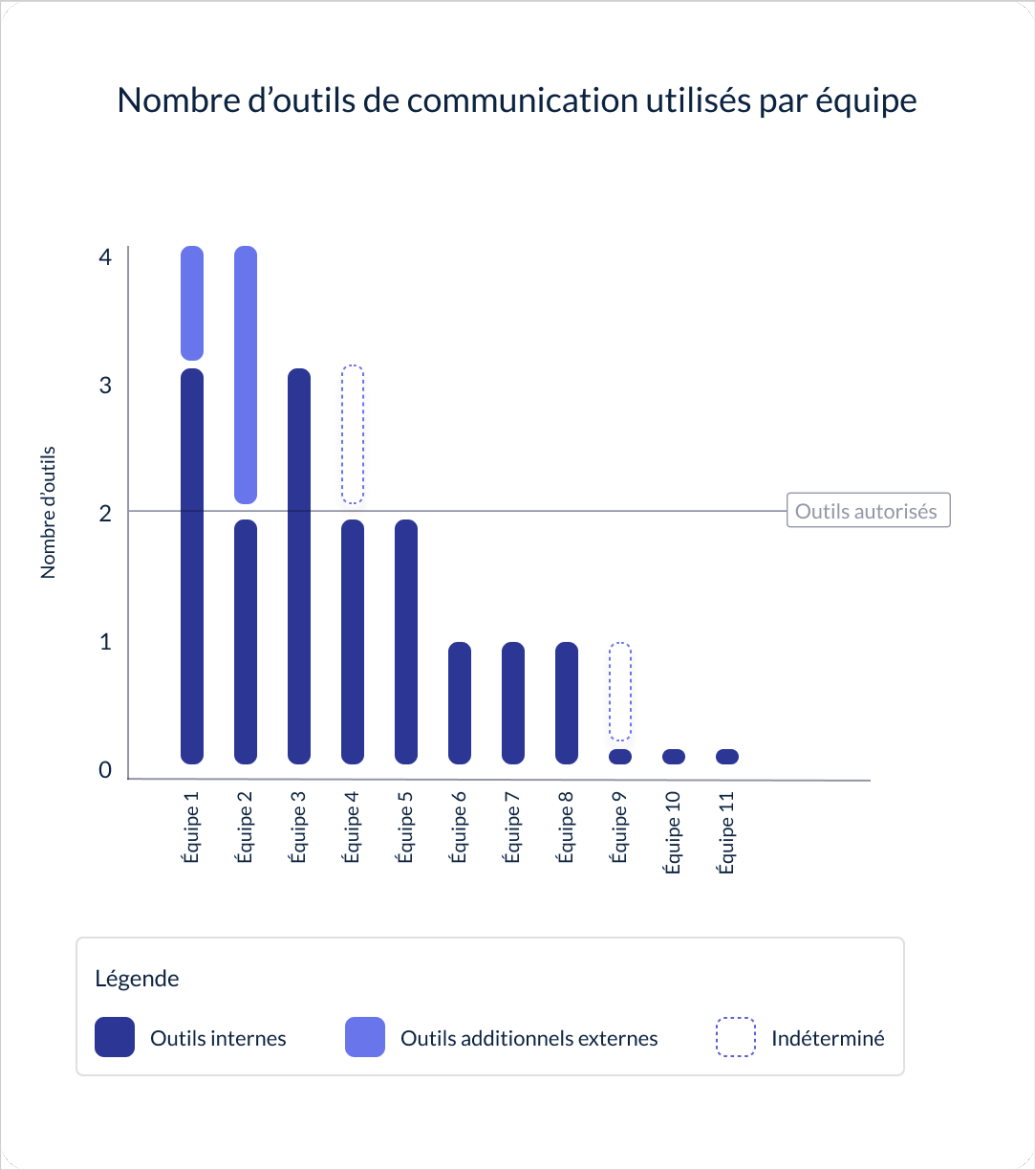

Figure 6.1 Nombre d'outils de communication utilisés

Une deuxième figure, soit la figure 6.2 présentée ci-après, présente les délais d'impacts significatifs sur les opérations, c'est-à-dire le moment précis où une perturbation passe d'un simple inconvénient à un problème majeur qui affecte la capacité de chaque équipe à accomplir ses tâches quotidiennes, à l'aide de barres de couleurs. L'outil de communication le plus critique et le pourcentage de télétravail de chaque équipe sont également indiqués à droite de la figure. Par exemple, le gestionnaire de l'équipe 1, dont l'équipe est en télétravail entre 25 % et 50 % du temps, a souligné que Teams était l'outil de communication le plus critique et que des impacts significatifs seraient ressentis immédiatement en cas d'indisponibilité des outils de communication. De son

côté, le gestionnaire de l'équipe 2, dont l'équipe travaille moins de 25 % du temps en télétravail, a également identifié Teams comme l'outil le plus critique, mais a précisé que les impacts significatifs sur les opérations de son équipe seraient ressentis entre une et deux heures après la perte des outils de communication. Les trois gestionnaires ayant affirmé n'utiliser aucun outil de communication dans leur équipe sont également illustrés au bas de la figure en gris, offrant une opportunité d'éclaircir ces informations durant l'atelier de validation. Somme toute, cette figure permet d'identifier au premier coup d'œil les outils de communication les plus critiques et de constater que, pour la majorité d'entre eux, les délais d'impact sont inférieurs à une journée et ce, que les équipes soient en télétravail ou en présentiel. Cette figure est ainsi conçue pour stimuler les échanges sur l'utilisation des outils de communication mais également sur les stratégies de continuité des activités correspondantes, en présentiel ou en télétravail.

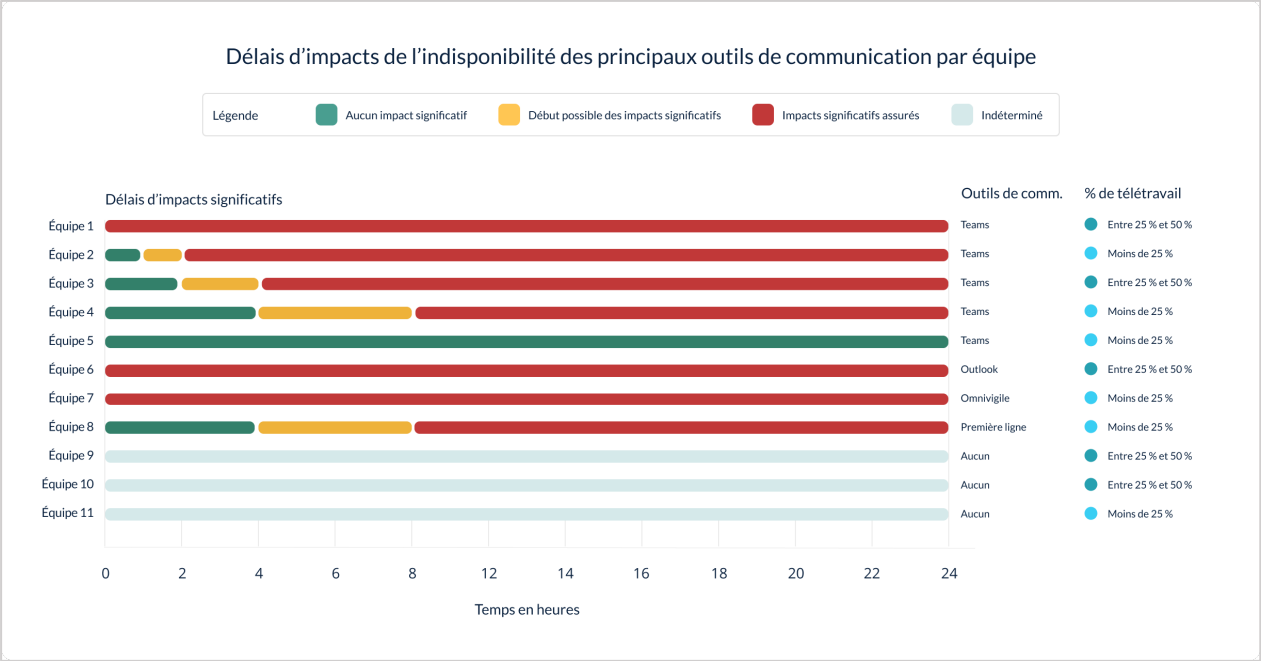

Figure 6.2 Impacts de l'indisponibilité des principaux outils de communication par équipe

Une dernière figure, relative à l'utilisation du logiciel ERP a été créée, celle-ci est présentée à la figure 6.3 ci-après. Nous avons choisi de dédier une figure au logiciel ERP puisque celui-ci est non seulement largement utilisé au sein de la municipalité, mais il est également exclusivement accessible via une connexion VPN en télétravail. Cette particularité offrait l'opportunité d'aborder ces aspects cruciaux liés aux modalités d'utilisation durant l'atelier de validation. La figure 6.3, organisée comme un tableau de bord sommaire, présente d'abord le taux d'utilisation du logiciel

ERP, qui est de 72 %. Elle montre également la répartition du télétravail au sein des équipes qui utilisent le logiciel ERP : 63 % travaillent moins de 25 % du temps en télétravail alors que 47 % se situent entre 25 % et 50 % du temps en télétravail. La figure illustre également le pourcentage de répondants ayant affirmé qu'une connexion VPN n'était pas nécessaire pour accéder au logiciel en télétravail, soit 12 %. Cette information contraste avec celle fournie par l'équipe TI, qui confirme la nécessité de la connexion VPN, et constitue ainsi un point de discussion pour l'atelier de validation. Enfin, la figure illustre les délais d'impacts significatifs de l'indisponibilité du logiciel ERP. Cela permet de comparer son importance à son utilisation en télétravail, conjointement avec le VPN, accentuant ainsi la vulnérabilité des opérations de la municipalité et favorisant les discussions sur les stratégies de continuité des activités. C'est donc 14 % des gestionnaires qui ont répondu que leur équipe ressentirait des impacts immédiats suite à l'indisponibilité du logiciel, 28 % entre une et deux heures, 14 % entre deux et quatre heures, et 44 % entre quatre et huit heures.

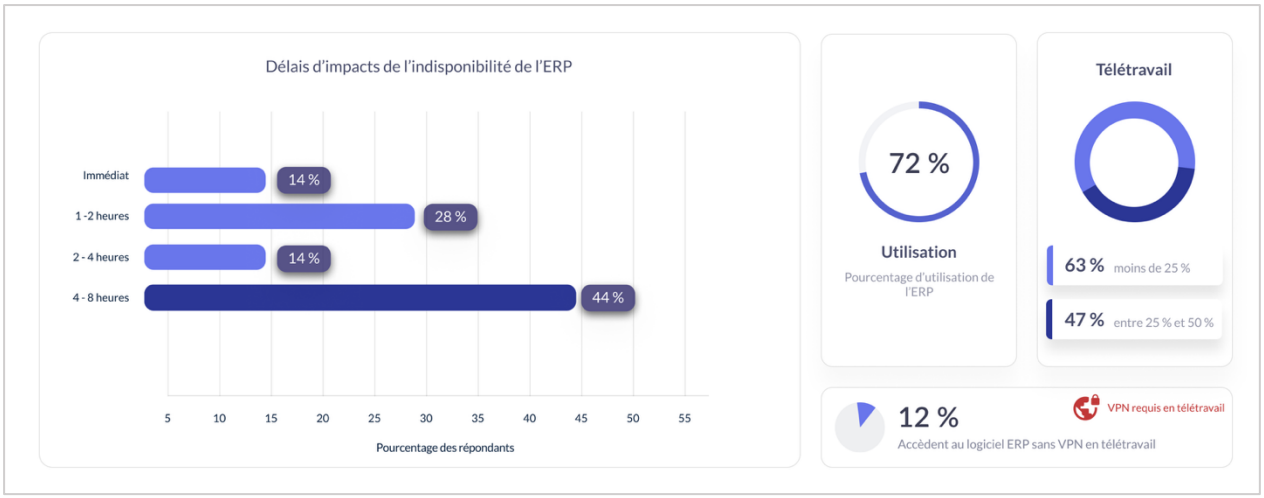

Figure 6.3 Informations sur l'utilisation de l'ERP

En général, l'analyse des réponses au questionnaire qui avait été transmis aux gestionnaires a révélé que les questions sur les délais d'impacts ont été bien comprises par les répondants. Cependant, les questions concernant le nombre d'outils par type d'utilisation ont suscité des difficultés. Par exemple, pour les outils de communication, plusieurs répondants ont cité des logiciels que notre classification rangeait plutôt dans la catégorie des outils d'organisation ou de collaboration, comme SharePoint qui est surtout une plateforme pour la gestion de contenu et le partage de documents. Nous avons également noté un nombre important de réponses de type « Je ne sais pas ». Comme mentionné à la section 5.3.3., cela suggère soit un manque de clarté dans la catégorisation de

l'utilisation des logiciels de bureautique de type SaaS, soit un certain désintérêt pour la démarche, ou encore une incompréhension des questions.

6.1.3 Atelier de validation

L'atelier a réuni 7 gestionnaires de la municipalité, dans le but de valider les figures de l'ISC, et ultimement établir une compréhension commune de l'utilisation des logiciels de bureautique de type SaaS, et de leur environnement technologique. Pour mieux répondre aux besoins exprimés par les représentants de la municipalité lors de la première rencontre, l'atelier avait également pour objectif de discuter des vulnérabilités des opérations face à l'utilisation de logiciels de bureautique de type SaaS, et d'échanger sur les stratégies de continuité à mettre en place.

Au niveau des figures en lien avec les outils de communication, les discussions ont principalement porté sur les stratégies de continuité à adopter en cas d'indisponibilité logiciels. Des solutions variées ont été évoquées par les gestionnaires, notamment le retour en présentiel et l'utilisation de solutions technologiques alternatives. Un constat majeur est apparu : bien que des initiatives existent en silo, aucune mesure de repli n'est actuellement systématisée, documentée ou communiquée à l'ensemble des gestionnaires de la municipalité. La discussion a également mis en lumière l'importance cruciale de l'équipe TI, dont la charge de travail semble très élevée et pour laquelle une absence de redondance a été notée. Nous avons observé une tendance générale à privilégier les solutions technologiques en cas de perturbation, plutôt que d'explorer des solutions plus opérationnelles ou procédurales. Par exemple, autant lors du premier atelier que de cet exercice de validation, les discussions autour des outils de communication convergeaient vers le déploiement de solutions technologiques équivalentes, comme le remplacement temporaire d'Outlook par Gmail. La réflexion s'orientait rarement vers une adaptation temporaire des opérations, une modification des méthodes de travail ou la documentation de procédures de remplacement.

La deuxième partie de l'atelier a porté sur la validation de la figure relative au logiciel ERP. Malgré les impacts potentiels liés à l'indisponibilité de l'outil, un consensus s'est dégagé parmi les gestionnaires sur la possibilité d'effectuer manuellement les opérations normalement accomplies via le logiciel ERP en cas de perturbation. Cependant, il a été noté que les procédures manuelles, bien qu'existantes, n'avaient pas été mises à jour récemment et, surtout, n'étaient pas facilement accessibles par toutes les équipes. Les participants à l'atelier ont également reconnu que pour les

nouveaux employés n'ayant jamais effectué ces tâches manuellement, la courbe d'apprentissage serait plus ardue. Considérant que les résultats ont démontré que l'ensemble des équipes seraient affectées dans les huit heures suivant l'indisponibilité de l'outil ERP, il nous apparaît optimiste de considérer les procédures manuelles comme une mesure de repli efficace. Finalement, le groupe a reconnu que l'indisponibilité de ce logiciel n'avait pas été pleinement anticipée et que les solutions de repli n'étaient pas formalisées et diffusées aux gestionnaires. Par conséquent, l'atelier a mis en évidence des vulnérabilités des opérations dues à l'utilisation des logiciels de communication et d'organisation, ainsi qu'un besoin pressant de formaliser les stratégies de continuité.

Bien que notre équipe de recherche ne puisse valider la façon dont les enjeux discutés pendant l'atelier seront adressés au sein de la municipalité, nous avons partagé les recommandations suivantes :

- Systématiser les plans de repli pour les outils de communication, en documentant les procédures et en les diffusant aux gestionnaires, en gardant l'équipe TI impliquée tout au long du processus.
- Mettre à jour et rendre accessibles les procédures manuelles pour les opérations critiques du logiciel ERP.
- Renforcer la résilience de l'équipe TI et évaluer des solutions opérationnelles en complément des approches technologiques pour la continuité.
- Sensibiliser et former l'ensemble du personnel aux plans de continuité, en insistant sur les procédures spécifiques au télétravail.

6.2 Validation des bases de l'ISC

L'exercice de validation nous a permis de confirmer plusieurs bases de l'ISC. Premièrement, par l'analyse des réponses au questionnaire et l'observation des échanges pendant l'atelier de validation, nous avons été en mesure de confirmer que les logiciels d'application constituent un point de référence commun qui est bien compris par les gestionnaires, l'équipe de continuité et l'équipe TI. Ces logiciels restent par conséquent des candidats pertinents et centraux à la démarche. En second lieu, l'exercice de validation nous a permis de confirmer la pertinence d'orienter la démarche sur les logiciels de bureautique de type SaaS. Comme lors du premier atelier, nous avons

constaté que les stratégies de continuité dédiées à ce type de logiciel sont pratiquement inexistantes, même si leur indisponibilité peut engendrer des impacts significatifs sur les activités à court terme.

Concernant les trois dimensions de l'ISC, plusieurs points sont ressortis clairement de l'exercice de validation :

- Type d'utilisation :
    - Nous avons constaté que cette dimension peut prêter à confusion. Les réponses aux questionnaires et les échanges durant l'atelier ont démontré que les gestionnaires ne différencient pas toujours clairement et uniformément les logiciels de communication, d'organisation et de collaboration. Par exemple, alors que certains gestionnaires considèrent SharePoint comme un outil de communication, d'autres le considèrent comme un outil d'organisation ou de collaboration.
    - L'exercice de validation a confirmé notre constat du chapitre 3 concernant un manque de détails cruciaux sur l'utilisation des logiciels ; cependant, le questionnaire n'a été que partiellement efficace pour recueillir ces informations. Le fait que certains logiciels puissent être utilisés à plusieurs fins et qu'il y ait des recoupements de fonctionnalités complexifie encore davantage la caractérisation et le dénombrement des outils, rendant ainsi la discussion sur le *Shadow IT* moins précise.
- Modalité d'utilisation : les réponses aux questionnaires nous ont permis de confirmer la pertinence d'aborder cette dimension, notamment en raison des confusions identifiées concernant la connexion VPN en télétravail.
- Portée d'utilisation : les discussions générées par l'atelier de validation ont confirmé la pertinence d'étudier cette dimension. Lors du premier atelier de validation, nous avions détecté que l'aspect « externe » n'avait pas été systématiquement considéré dans les stratégies de continuité des activités des participants. Dans cet exercice de validation, nous avons fait l'observation inverse : certains gestionnaires semblent avoir réfléchi aux stratégies de continuité relativement aux communications externes, avec les citoyens, mais aucune stratégie de continuité ne semble être en place pour les communications internes.

En somme, l'exercice de validation a confirmé que nos trois dimensions constituaient de bons angles pour explorer l'utilisation de logiciels de bureautique de type SaaS et de leur environnement

technologique. Cependant, comme observé lors du premier atelier et confirmé par cet exercice de validation, ces dimensions doivent absolument être adaptées au contexte technologique de l'organisation.

6.3 Retours sur la démarche proposée

Dans le cadre de l'exercice de validation, la démarche a révélé son potentiel pour enrichir les connaissances communes sur l'environnement technologique et son utilisation au sein de la municipalité. Pour les gestionnaires, l'analyse de l'utilisation des logiciels de bureautique de type SaaS au sein de leur équipe, suivie d'une discussion collective lors de l'atelier de validation, a permis d'approfondir leurs connaissances et leur compréhension commune de cette utilisation à travers l'organisation. Parallèlement, la planification de la collecte d'information, la validation du questionnaire et l'analyse des réponses ont permis aux membres de l'équipe ISC de converger vers une vision partagée de l'utilisation des logiciels de bureautique de type SaaS, stimulant ainsi la collaboration. C'est précisément cette dynamique d'enrichissement et de partage des connaissances qui nous a conduit à une réalisation fondamentale, renforçant ainsi les conclusions du premier atelier : la démarche a forcé une prise de conscience collective quant à l'importance des logiciels de bureautique de type SaaS et à la vulnérabilité des opérations de l'organisation face à leur utilisation. Cette prise de conscience collective, observable lors des échanges du premier atelier et confirmée par l'exercice de validation, a mené les participants à constater l'absence ou le manque de formalisation des mesures de repli existantes pour les logiciels de bureautique de type SaaS. Cette révélation a agi comme un puissant catalyseur, générant des discussions animées autour des actions concrètes à engager pour pallier ces vulnérabilités.

Malgré les apports positifs de la démarche, une observation majeure ressort de l'exercice de validation : l'équipe ISC doit travailler en collaboration étroite, de façon continue et intégrée, pour recueillir les informations et pour créer l'ISC. Dans le cadre de notre exercice de validation, l'équipe ISC s'est rencontrée à deux reprises pour valider le questionnaire, après quoi notre équipe de recherche a pris en charge une grande portion du travail lié à la collecte d'informations et à la création de l'ISC. Nos connaissances limitées de l'environnement technologique de la municipalité, combinées à une création de l'ISC qui s'est effectuée partiellement en silo, ont contribué à diminuer légèrement l'efficacité de la démarche. Somme toute, bien que l'atelier de validation reste essentiel pour établir la compréhension commune de l'environnement

technologique recherchée, c'est aussi l'analyse des réponses au questionnaire, la mise en commun des informations, l'identification des informations clés, la structuration de l'ISC et la création des figures qui stimulent la réflexion des intervenants impliqués dans l'équipe ISC et qui contribuent à solidifier la collaboration.

L'étape 2 de notre démarche, axée sur la caractérisation préliminaire, s'est également avérée insuffisante pour fournir les connaissances approfondies des logiciels de bureautique de type SaaS et de l'environnement technologique de la municipalité, spécifiquement dans notre contexte où l'équipe ISC est composée, en partie, d'une équipe externe comme la nôtre. Cette connaissance des logiciels de bureautique de type SaaS et de leur environnement technologique est essentielle pour créer l'ISC et animer l'atelier de validation efficacement. En effet, comme l'atelier vise à établir une compréhension commune de l'environnement technologique et de son utilisation et qu'il réunit des participants ayant des champs de compétences qui présentent peu de points d'intersection, l'animateur doit être en mesure d'apporter les précisions nécessaires pour assurer la compréhension de tous et poser des questions pertinentes afin de guider les échanges. Cette tâche est mieux accomplie lorsque l'animateur possède une connaissance approfondie de l'environnement technologique et de son utilisation dans l'organisation.

6.4 Recommandations

Bien que la démarche ait prouvé son efficacité pour initier des discussions essentielles pour améliorer la compréhension commune de l'environnement technologique et son utilisation et ainsi mieux cerner la vulnérabilité des opérations de l'organisation, certains aspects de son exécution pourraient être perfectionnés pour en améliorer l'efficacité.

Tout d'abord, comme mentionné à la section 6.2, la dimension « type d'utilisation » a porté à confusion chez certains répondants. Pour pallier ce problème, il serait pertinent de préciser les types d'utilisation en orientant les questions vers des groupes de fonctionnalités plus spécifiques. Au lieu de fournir une description générique de chaque type d'utilisation et de poser des questions génériques quant à leur utilisation, celles-ci pourraient être plus précises et axées sur des grands groupes de fonctionnalités. Par exemple, pour un logiciel de collaboration, la question pourrait être : « Votre équipe utilise-t-elle des logiciels pour éditer des fichiers de façon collaborative avec d'autres équipes à l'interne ? » au lieu de : « Votre équipe utilise-t-elle des outils pour collaborer

en interne ? ». Ces questions légèrement plus précises pourraient améliorer la compréhension des types d'utilisation et ainsi améliorer la qualité des réponses.

En second lieu, comme exploré dans la section précédente, l'exercice de validation a démontré qu'il est crucial que tous les membres de l'équipe ISC participent activement aux étapes 1 à 4, de la planification de la collecte d'information jusqu'à la création de l'ISC. En effet, la réflexion qui sous-tend la création de l'ISC est essentielle à la pleine efficacité de la démarche. Pour ce faire, nous recommandons qu'une équipe ISC dédiée soit assignée à cette démarche par l'organisation et que ses membres aient dégagé le temps nécessaire pour s'y consacrer pleinement. Nous recommandons par ailleurs que cette équipe de travail soit pérennisée et qu'un horaire de mise à jour de l'ISC soit fixé dès l'étape 1 de la démarche. Cela lui permettrait non seulement de prendre en charge la mise à jour continue de l'ISC, solidifiant ainsi une collaboration à long terme, mais aussi d'atténuer le fossé qui se creuse naturellement entre les équipes au fil du temps. Enfin, cette équipe pérenne serait la mieux placée pour s'assurer que les retombées de la démarche soient concrétisées en actions tangibles.

Nous recommandons également que l'équipe ISC prépare des points de discussion spécifiques pour animer les échanges lors de l'atelier de validation. Ces points varieront évidemment en fonction de l'ISC élaborée et des besoins particuliers de l'organisation. Cependant, deux observations clés issues de notre premier atelier et de l'exercice de validation méritent une attention particulière :

- Diversifier les solutions de repli : comme mentionné à la section précédente, les participants tendent naturellement à privilégier des mesures de repli technologiques pour remplacer un logiciel indisponible. Dans un contexte où les équipes TI sont souvent surchargées, il est pertinent de guider la discussion afin d'encourager une réflexion approfondie sur des solutions opérationnelles ou procédurales.
- Aligner les délais d'impact et les stratégies de continuité : tant lors du premier atelier que de l'exercice de validation, nous avons constaté un décalage entre le temps moyen où les équipes commencent à ressentir des impacts significatifs dus à l'indisponibilité des logiciels et le temps d'implémentation des solutions de repli proposées. Bien que le rôle de l'animateur ne soit pas d'imposer un constat, il est essentiel qu'il puisse orienter les discussions vers une prise de conscience des disparités.

- Démystifier le contrôle de l'équipe TI : nous avons constaté un flou persistant concernant le rôle et le niveau de contrôle de l'équipe TI sur les logiciels d'application, notamment les logiciels de type SaaS, à travers les différentes équipes. Les discussions devraient donc être guidées pour éclaircir ce point lorsque l'opportunité se présente.

6.5 Suite du projet

Cette étude nous a permis de confirmer un besoin pressant dans la majorité des organisations : celui de mieux comprendre l'environnement technologique et son utilisation, de mieux cerner les vulnérabilités et ultimement, d'améliorer la préparation aux perturbations. À cette fin, les réflexions et discussions amorcées grâce à la démarche proposée constituent un excellent point de départ pour établir cette compréhension commune, et ainsi assurer une collaboration solide entre les gestionnaires, l'équipe de continuité et l'équipe TI.

Afin de valider la robustesse de cette démarche prometteuse et de formaliser son adaptabilité à divers contextes, il serait pertinent d'exécuter des exercices de validation supplémentaires auprès d'une variété d'organisations. Pour ce faire, nous suggérons de cibler différents types d'organisations :

- Organisations à utilisation intensive de logiciels d'application : il serait bénéfique d'inclure des organisations qui utilisent intensivement les logiciels d'application, particulièrement les outils d'organisation et de collaboration puisque ces derniers n'ont pu être couverts pleinement lors de notre exercice de validation.
- Organisations de plus grande taille : tester la démarche avec des organisations de plus grande taille permettrait d'évaluer son extensibilité et de documenter les méthodes pour la moduler à des organisations de toutes dimensions.
- Organisations issues de divers secteurs économiques : cela aiderait à évaluer la polyvalence de l'approche et à documenter comment elle peut être adaptée à différents secteurs d'activité, dans le secteur public ou privé.
- Organisations dotées d'une équipe de continuité dédiée : observer l'impact de la démarche dans des organisations qui disposent déjà de stratégies de continuité détaillées, ce qui n'était pas le cas dans notre exercice de validation, fournirait des aperçus précieux sur les retombées potentielles de la démarche.

Tester la démarche dans ces contextes variés permettrait non seulement de la raffiner, mais aussi de formaliser un processus pour l'adapter à tout type d'organisation. Voici quelques exemples de la façon dont la démarche pourrait être adaptée :

- Les trois dimensions explorées pourraient être élargies, et des procédures pour les ajuster au contexte spécifique de chaque organisation pourraient être formalisées. Par exemple, de nouveaux types d'utilisation pourraient être ajoutés et les modalités et la portée d'utilisation pourraient être explorées sous des angles différents.
- Des dimensions pourraient être ajoutées afin de remplacer les dimensions qui ne sont pas applicables. L'ISC doit rester simple et facilement compréhensible, nous recommandons donc de la maintenir à trois dimensions. Cependant, il est possible que certaines des dimensions explorées dans cette étude ne soient pas entièrement applicables à une organisation et qu'elles puissent être remplacées par de nouvelles dimensions. Il serait pertinent de documenter ce processus.
- La démarche, qui se concentre actuellement sur les logiciels de bureautique de type SaaS, pourrait également être étendue à d'autres types de logiciels d'application, comme par exemple des outils d'intelligence artificielle. Nous recommandons toutefois de conserver le logiciel d'application comme sujet principal de l'étude, puisqu'il a été confirmé qu'il restait un point de référence commun pour tous les intervenants.

Finalement, il serait également essentiel de reproduire l'exercice de validation avec une organisation ayant la capacité d'assigner une équipe ISC permanente et d'y allouer le temps nécessaire. Cela permettrait de constater les impacts de la démarche à plus long terme et d'évaluer et de documenter si elle contribue à améliorer et aligner les stratégies de continuité. Il pourrait même être envisageable de documenter des processus pour convertir les retombées de la démarche en actions tangibles.

CHAPITRE 7 CONCLUSION

Ce projet de recherche propose une démarche qui répond au constat initial : les gestionnaires, l'équipe de continuité et l'équipe TI ne possèdent pas systématiquement de compréhension commune de l'environnement technologique de l'organisation et de son utilisation. Cette absence de synergie peut mener à une collaboration difficile et à un manque d'alignement dans les activités de préparation aux perturbations.

Pour adresser ce défi crucial, notre démarche s'est appuyée sur les recherches du Centre risque & performance qui préconisent la création et la validation d'une ISC comme mécanisme pour améliorer la compréhension commune et ainsi favoriser la collaboration entre les équipes, dans un contexte de préparation à des perturbations. Sur la base de nos connaissances techniques et de notre expérience professionnelle, nous avons sélectionné les logiciels d'application – plus précisément les logiciels de bureautique de type SaaS – comme point central de l'ISC, majoritairement pour leur caractère stratégique en tant que point de référence commun entre les équipes. Nous avons défini des dimensions de l'ISC qui permettent d'obtenir une perspective holistique de l'environnement technologique et de son utilisation : le type d'utilisation, les modalités d'utilisation et la portée d'utilisation. Ces dimensions ont par la suite été validées lors d'un premier atelier.

C'est en nous appuyant sur ces fondations solides que nous avons été en mesure de proposer une démarche pour initier une approche collaborative, centrée sur la création et la validation d'une ISC. Cette démarche a ensuite été testée lors d'un exercice de validation. L'atelier de validation proposé dans la démarche a prouvé son efficacité pour initier des discussions qui ont contribué à améliorer les connaissances et la compréhension commune de l'environnement technologique et de son utilisation chez les participants. Néanmoins, c'est la création de l'ISC elle-même qui s'est avérée être l'étape la plus cruciale pour bâtir une collaboration solide entre l'équipe de continuité et l'équipe TI. En effet, la démarche a permis aux deux équipes de travailler ensemble, dans un court laps de temps, pour analyser les besoins de l'organisation en matière de préparation aux perturbations et réfléchir aux lacunes potentielles dans la compréhension de l'environnement technologique et de son utilisation. Cette réflexion collective, qui a servi de base pour la structuration de la collecte d'information et de l'ISC, a favorisé de riches échanges et la création de points de référence communs. Tout au long du processus, les membres de l'équipe ISC ont donc

eu l’occasion de travailler ensemble pour améliorer leurs propres connaissances et ultimement, mieux se comprendre.

En plus de reconfirmer nos hypothèses et de valider la pertinence de la démarche, l’exercice de validation nous a également permis de formuler des recommandations et des principes de conception pour la raffiner, ces derniers pouvant être pris en compte dans de futures itérations. Finalement, nous avons pu explorer comment cette étude peut servir de tremplin pour d’autres exercices de validation, afin de raffiner davantage la démarche et de la rendre plus adaptable.

RÉFÉRENCES

Adger, W. N. (2006). Vulnerability. *Global Environmental Change*, *16*(3), 268-281. https://doi.org/10.1016/j.gloenvcha.2006.02.006

Application software. (2025). Dans *Britannica*. https://www.britannica.com/technology/application-software

Atlassian. (s. d.). *Calculating the cost of downtime*. Atlassian. Consulté 15 mai 2025, à l'adresse https://www.atlassian.com/incident-management/kpis/cost-of-downtime

Banque de développement du Canada. (s. d.). *Que sont les opérations*. BDC.ca. Consulté 16 avril 2025, à l'adresse https://www.bdc.ca/fr/articles-outils/boite-outils-entrepreneur/gabarits-documents-guides-affaires/glossaire/operations

Banque de développement du Canada. (2022, avril). *Adopter le numérique, qu'est-ce que c'est?* BDC.ca. https://www.bdc.ca/fr/articles-outils/technologie/investir-technologie/adopter-numerique-quest-ce-que-cest

BetterCloud. (2020). *2020 State of SaaSOps*.

Canadian Remote Work Statistics and Trends 2025. (2025, juin 2). Robert Half Canada. https://www.roberthalf.com/ca/en/insights/research/canadian-remote-work-statistics-and-trends

Cardona, O. (2004). The Need for Rethinking the Concepts of Vulnerability and Risk from a Holistic Perspective : A Necessary Review and Criticism for Effective Risk Management. *Mapping Vulnerability. Disasters, Development and People*.

Centre canadien pour la cybersécurité, G. du C. (2021, janvier 14). *Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)*. https://www.cyber.gc.ca/fr/orientation/elaboration-dun-plan-de-reprise-informatique-personnalise-itsap40004

Charmont, E. (2025). *La résilience organisationnelle ou une gestion collaborative et adaptative des perturbations*. Polytechnique Montréal.

COVID-19 digital transformation & technology | McKinsey. (s. d.). Consulté 4 avril 2025, à l'adresse https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-

insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

Dempsey, K., Eavy, P., Moore, G., & Takamura, E. (2019). *Automation Support for Security Control Assessments : Software Vulnerability Management*. https://doi.org/10.6028/NIST.IR.8011-4-draft

DevX. (2023). *Application Software—Glossary*. https://www.devx.com/terms/application-software/

Do, V., McBrien, H., Flores, N. M., Northrop, A. J., Schlegelmilch, J., Kiang, M. V., & Casey, J. A. (2023). Spatiotemporal distribution of power outages with climate events and social vulnerability in the USA. *Nature Communications*, *22*. https://www.nature.com/articles/s41467-023-38084-6

Faivre, N. (2021). *Étude sur la cybersécurité et les opportunités offertes par l'accès aux données au Québec*. Fédération des chambres de commerce du Québec; Collections de BAnQ. https://numerique.banq.qc.ca/patrimoine/details/52327/4643893

Gilbert Roussel, U. M. (2024). *Espace de résilience dédié à la gestion des conséquences sur des acteurs économiques sur un territoire*. Polytechnique Montréal.

Gouvernement du Canada, S. C. (2023, juillet 28). *Adoption des technologies de pointe additionnelles, selon l'industrie et la taille de l'entreprise*. https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=2710037001

Gouvernement du Québec. (2016). *Portrait de la main-d'oeuvre en technologies de l'information de la fonction publique du Québec 2015*. Direction des communications du Secrétariat du Conseil du trésor.

Gouvernement du Québec. (2018). *Résultats du sondage sur la gestion de la continuité des activités*. Gouvernement du Québec. https://www.quebec.ca/securite-situations-urgence/urgences-sinistres-risques-naturels/entreprise/resultats-sondage-gestion-continuite-activites

Gouvernement du Québec. (2024, avril 12). *Part des entreprises qui utilisent des outils de communication et de travail collaboratif (technologies sélectionnées), Québec*. Institut de la statistique du Québec. https://statistique.quebec.ca/fr/produit/tableau/3566

Haranas, M. (2025, mai 5). *Microsoft Vs. AWS Vs. Google Cloud Earnings Q1 2025 Face-Off*. https://www.crn.com/news/cloud/2025/microsoft-vs-aws-vs-google-cloud-earnings-q1-2025-face-off

Harvard Business Review. (2021). Accelerating Forward : The State of Cloud-Driven Transformation. *Harvard Business Review*, 10.

Hoory, L. (2023, mars 8). *The State Of Workplace Communication*. Forbes Advisor. https://www.forbes.com/advisor/business/digital-communication-workplace/

ISO 17757:2019. (2019). https://www.iso.org/obp/ui/en/#iso:std:iso:17757:ed-2:v1:en

Jones, E. (2020, mai 4). Types of Cloud Computing : An Extensive Guide on Cloud Solutions and Technologies. *Kinsta®*. https://kinsta.com/blog/types-of-cloud-computing/

Lawrence, A., & Simon, L. (2023). *Annual outage analysis 2023 : The causes and impacts of IT and data center outages*.

LeanIX. (s. d.). *SaaS Management : Le Guide ultime | LeanIX*. Consulté 5 avril 2025, à l'adresse https://www.leanix.net/fr/wiki/apm/saas-management

Ledwith, A., & Ludden, P. (2016). A Typology Framework for Virtual Teams. *PMI Sponsored Research*. https://www.pmi.org/learning/library/typology-framework-virtual-teams-11197

Microsoft Azure. (s. d.). *What is Software as a Service (SaaS)? | Microsoft Azure*. Consulté 5 avril 2025, à l'adresse https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas

Office de la langue française. (s. d.). *Vulnérabilité informatique*. Gouvernment du Québec. Consulté 5 avril 2025, à l'adresse https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8354651/vulnerabilite-informatique

Paerata, K. (2023). The use of workplace instant messaging since COVID-19. *Telematics and Informatics Reports*, *10*, 100063. https://doi.org/10.1016/j.teler.2023.100063

PC Matic. (2021). *Cybersecurity in the Remote Workforce*.

Red Hat. (2022). *What is middleware?* https://www.redhat.com/en/topics/middleware/what-is-middleware

Sargut, G., & McGrath, R. (2011). Learning to Live with Complexity. *Harvard Business Review*. https://hbr.org/2011/09/learning-to-live-with-complexity

Spotlight on shadow IT. (2023, juillet 27). National Cyber Security Center. https://www.ncsc.gov.uk/blog-post/spotlight-on-shadow-it

Statistiques Canada. (2024, mai 27). *Technologies the business or organization plans to adopt or incorporate over the next 12 months, second quarter of 2024*. https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3310082201

Suarez, P. (2002). *Urbanization, climate change and flood risk : Addressing the fractal nature of differential vulnerability*.

The Business Continuity Institute. (2018). *Guide de bonnes pratiques*. The Business Continuity Institute.

The Business Continuity Institute. (2023). *BCI Continuity and Resilience Report 2023* (p. 104).

U.S. Air Force. (2021, octobre 3). *Air Force Doctrine*.

Usito. (s. d.). *Usito*. Usito. Consulté 7 avril 2025, à l'adresse https://usito.usherbrooke.ca

What is System Software? | Definition from TechTarget. (s. d.). WhatIs. Consulté 4 avril 2025, à l'adresse https://www.techtarget.com/whatis/definition/system-software

World Economic Forum. (2020). *The Future of Jobs Report 2020*. https://www.weforum.org/publications/the-future-of-jobs-report-2020/in-full/2-1-technological-adoption/

ANNEXE A EXEMPLE DE QUESTIONNAIRE POUR LES GESTIONNAIRES

Portrait de l'utilisation des technologies numériques

Ce questionnaire comprend des questions haut niveau relativement aux technologies numérique de communication, d'organisation et de collaboration qui sont utilisées au sein de votre équipe.

Vous devriez compter approximativement 3 à 5 minutes pour remplir ce questionnaire.

Quel est le pourcentage approximatif du travail accompli en télétravail dans votre équipe?

- Moins de 25%
- Entre 25% et 50%
- Entre 50% et 75%
- Plus de 75%
- Je ne sais pas

Est-ce que l'utilisation de certains logiciels nécessitent obligatoirement une connexion à un réseau privé sécurisé (ex. : VPN)?

- Oui
- Non
- Je ne sais pas

Votre équipe utilise-t-elle [NOM DU ERP]

- Oui
- Non
- Je ne sais pas

Outils de communication

Cette section du questionnaire concerne les technologies numériques que vous utilisez pour transmettre et recevoir des messages à l'interne et à l'externe.

Votre équipe utilise-t-elle des technologies numériques pour communiquer à l'interne?

- Oui, plusieurs technologies numériques
- Oui, une technologie numérique
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de technologies numériques

Votre équipe utilise-t-elle des technologies numériques additionnelles pour communiquer avec des équipes externes, par exemple des fournisseurs ou des clients?

- Oui, plusieurs technologies numériques
- Oui, une technologie numérique
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de technologies numériques

Outils d'organisation

Cette section du questionnaire concerne les outils de gestion, de coordination ou de planification des tâches, des activités, des processus et des ressources à l'interne et à l'externe.

Votre équipe utilise-t-elle des technologies numériques pour organiser le travail à l'interne?

- Oui, plusieurs technologies numériques
- Oui, une technologie numérique
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de technologies numériques

Votre équipe utilise-t-elle des technologies numériques additionnelles pour organiser le travail en rapport avec des équipes externes, par exemple des fournisseurs ou des clients?

- Oui, plusieurs technologies numériques
- Oui, une technologie numérique
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de technologies numériques

Est-ce que l'utilisation de certaines de ces technologies numériques nécessitent obligatoirement une connexion à un réseau privé sécurisé (ex. : VPN)?

- Oui, plusieurs technologies numériques
- Oui, une technologie numérique
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de technologies numériques

Outils de collaboration

Cette section du questionnaire concerne les principaux outils qui vous permettent de partager un fichier à l'interne ou à l'externe, ainsi que de le consulter et le modifier simultanément.

Votre équipe utilise-t-elle des technologies numériques pour travailler de façon collaborative à l'interne?

- Oui, plusieurs technologies numériques
- Oui, une technologie numérique
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de technologies numériques

Votre équipe utilise-t-elle des technologies numériques additionnelles pour travailler de façon collaborative avec des équipes externes, par exemple des fournisseurs ou des clients?

- Oui, plusieurs technologies numériques
- Oui, une technologie numérique
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de technologies numériques

Est-ce que l'utilisation de certaines de ces technologies numériques nécessitent obligatoirement une connexion à un réseau privé sécurisé (ex. : VPN)?

- Oui, plusieurs technologies numériques
- Oui, une technologie numérique
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de technologies numériques

ANNEXE B EXEMPLE DE QUESTIONNAIRES POUR L'ÉQUIPE TI

Portrait de l'utilisation des technologies numériques

Ce questionnaire comprend des questions haut niveau relativement aux logiciels de communication, d'organisation et de collaboration utilisés dans votre entreprise.

Vous devriez compter approximativement 3 à 5 minutes pour remplir ce questionnaire.

Les utilisateurs en télétravail doivent-t-ils obligatoirement se connecter à un réseau privé sécurisé (ex: VPN) pour accéder à certains logiciels?

- Oui
- Non
- Je ne sais pas

Dans votre entreprise, globalement, vous estimez le pourcentage approximatif du travail accompli en télétravail à :

- Moins de 25%
- Entre 25% et 50%
- Entre 50% et 75%
- Plus de 75%
- Je ne sais pas

Outils de communication

Cette section du questionnaire concerne les principaux logiciels qui sont utilisés pour transmettre et recevoir des messages à l'interne et à l'externe de votre entreprise.

Est-ce que votre équipe a autorisé l'utilisation de certains logiciels de communication?

- Oui, plusieurs logiciels
- Oui, un logiciel
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de logiciel autorisés

Combien de ces logiciels sont utilisés par l'ensemble de l'entreprise?

Selon vous, est-ce que des logiciels de communication qui n'ont pas été autorisés par votre équipe sont utilisés dans votre entreprise?

- Oui, plusieurs logiciels
- Oui, un logiciel
- Non
- Je ne sais pas

Veuillez inscrire ici votre estimation du nombre de logiciels non approuvés

---

Outils d'organisation

Cette section du questionnaire concerne les principaux logiciels de gestion, de coordination ou de planification des tâches, des activités, des processus et des ressources de votre entreprise.

Est-ce que votre équipe a autorisé l'utilisation de certains logiciels d'organisation?

Oui, plusieurs logiciels Oui, un logiciel Non Je ne sais pas

Veuillez inscrire ici le nombre de logiciels autorisés

Combien de ces logiciels sont utilisés par l'ensemble de l'entreprise?

Selon vous, est-ce que des logiciels d'organisation qui n'ont pas été autorisés par votre équipe sont utilisés dans votre entreprise?

Oui, plusieurs logiciels Oui, un logiciel Non Je ne sais pas

Veuillez inscrire ici votre estimation du nombre de logiciels non approuvés

---

Outils de collaboration

Cette section du questionnaire concerne les principaux outils qui vous permettent de partager un fichier à l'interne ou à l'externe, ainsi que de le consulter et le modifier simultanément.

Est-ce que votre équipe a autorisé l'utilisation de certains logiciels de collaboration?

Oui, plusieurs logiciels Oui, un logiciel Non Je ne sais pas

Veuillez inscrire ici le nombre de logiciels autorisés

Combien de ces logiciels sont utilisés par l'ensemble de l'entreprise?

Selon vous, est-ce que des logiciels de collaboration qui n'ont pas été autorisés par votre équipe sont utilisés dans votre entreprise?

Oui, plusieurs logiciels Oui, un logiciel Non Je ne sais pas

Veuillez inscrire ici votre estimation du nombre de logiciels non approuvés

ANNEXE C QUESTIONNAIRE POUR L'EXERCICE DE VALIDATION

Portrait de l'utilisation des technologies numériques dans votre équipe

Ce questionnaire comprend des questions relativement aux logiciels de communication, d'organisation et de collaboration qui sont utilisés au sein de votre équipe.

Vous devriez compter approximativement 5 minutes pour remplir ce questionnaire.

Quel est le pourcentage approximatif du travail effectué en télétravail dans votre équipe?

- Moins de 25%
- Entre 25% et 50%
- Entre 50% et 75%
- Plus de 75%
- Je ne sais pas

Votre équipe utilise-t-elle le logiciel ERP?

- Oui
- Non
- Je ne sais pas

En télétravail, devez-vous vous connecter au VPN pour accéder à ce logiciel?

- Oui
- Non
- Je ne sais pas

Si ce logiciel devenait indisponible, au bout de combien de temps les activités de votre équipe seraient-elles significativement affectées?

- Immédiatement
- Entre 1 et 2 hr
- Entre 2 et 4 hr
- Entre 4 et 8 hr
- Autre _____

Outils de communication

Cette section du questionnaire concerne les logiciels que vous utilisez pour transmettre et recevoir des messages, en interne et à l'externe, avec des fournisseurs ou des partenaires.

Votre équipe utilise-t-elle des logiciels pour communiquer à l'interne?

- Oui, plusieurs logiciels
- Oui, un logiciel
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de logiciels

Votre équipe utilise-t-elle des logiciels additionnels pour communiquer avec des équipes externes, par exemple des fournisseurs ou des partenaires?

- Oui, plusieurs logiciels
- Oui, un logiciel
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de logiciels

Parmi les logiciels de communication utilisés, lequel est le plus critique pour le bon déroulement des activités de votre équipe?

Si vos principaux logiciels de communication devenaient indisponibles, au bout de combien de temps les activités de votre équipe seraient-elles significativement affectées?

- Immédiatement
- Entre 1 et 2 hr
- Entre 2 et 4 hr
- Entre 4 et 8 hr
- Autre _____

Outils d'organisation et de collaboration

Cette section concerne vos logiciels d'organisation (planification, gestion des tâches et ressources) et de collaboration (partage et modification simultanée de fichiers), utilisés en interne comme avec des partenaires externes.

Votre équipe utilise-t-elle des logiciels pour collaborer à l'interne?

- Oui, plusieurs logiciels
- Oui, un logiciel
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de logiciels utilisés

Votre équipe utilise-t-elle des logiciels additionnels pour collaborer avec des équipes externes, par exemple des fournisseurs ou des partenaires?

- Oui, plusieurs logiciels
- Oui, un logiciel
- Non
- Je ne sais pas

Veuillez inscrire ici le nombre de logiciels utilisés

En télétravail, devez-vous vous connecter au VPN pour accéder à ces logiciels?

- Oui, pour tous ces logiciels
- Oui, pour plusieurs logiciels
- Non
- Je ne sais pas

Si vous avez répondu plusieurs logiciels, veuillez inscrire ici le nombre de logiciels de collaboration qui nécessitent une connexion VPN en télétravail

Face à l'indisponibilité de tous vos outils d'organisation et de collaboration, après quel délai les activités de votre équipe seraient significativement affectées?

- Immédiatement
- Entre 1 et 2 hr
- Entre 2 et 4 hr
- Entre 4 et 8 hr
- Autre _____