| **Titre:** Title: | System health monitoring using a novel method : security unified process |
|---|---|
| **Auteurs:** Authors: | Alireza Shameli-Sendi, Masoume Jabbarifar, Michel Dagenais, & Mehdi Shajari |
| **Date:** | 2012 |
| **Type:** | Article de revue / Article |
| **Référence:** Citation: | Shameli-Sendi, A., Jabbarifar, M., Dagenais, M., & Shajari, M. (2012). System health monitoring using a novel method : security unified process. Journal of Computer Networks and Communications, 2012, 1-20. https://doi.org/10.1155/2012/151205 |

| **URL de PolyPublie:** PolyPublie URL: | https://publications.polymtl.ca/3644/ |
|---|---|
| **Version:** | Version officielle de l'éditeur / Published version Révisé par les pairs / Refereed |
| **Conditions d'utilisation:** Terms of Use: | CC BY |

## Document publié chez l'éditeur officiel
Document issued by the official publisher

| **Titre de la revue:** Journal Title: | Journal of Computer Networks and Communications (vol. 2012) |
|---|---|
| **Maison d'édition:** Publisher: | Hindawi |
| **URL officiel:** Official URL: | https://doi.org/10.1155/2012/151205 |
| **Mention légale:** Legal notice: | |

*Research Article*

# System Health Monitoring Using a Novel Method: Security Unified Process

**Alireza Shameli-Sendi,[1] Masoume Jabbarifar,[1] Michel Dagenais,[1] and Mehdi Shajari[2]**

[1] *Départment de Genie Informatique et Génie Logiciel, École Polytechnique de Montréal, P.O. Box 6079, Succ. Downtown, Montreal, QC, Canada H3C 3A7*

[2] *Department of Computer Engineering & Information Technology, Amirkabir University of Technology, 424 Hafez Avenue, Tehran, Iran*

Correspondence should be addressed to Alireza Shameli-Sendi, alireza.shameli-sendi@polymtl.ca

Iterative and incremental mechanisms are not usually considered in existing approaches for information security management System (ISMS). In this paper, we propose SUP (security unified process) as a unified process to implement a successful and high-quality ISMS. A disciplined approach can be provided by SUP to assign tasks and responsibilities within an organization. The SUP architecture comprises static and dynamic dimensions; the static dimension, or disciplines, includes business modeling, assets, security policy, implementation, configuration and change management, and project management. The dynamic dimension, or phases, contains inception, analysis and design, construction, and monitoring. Risk assessment is a major part of the ISMS process. In SUP, we present a risk assessment model, which uses a fuzzy expert system to assess risks in organization. Since, the classification of assets is an important aspect of risk management and ensures that effective protection occurs, a Security Cube is proposed to identify organization assets as an asset classification model. The proposed model leads us to have an offline system health monitoring tool that is really a critical need in any organization.

## 1. Introduction

Information security is a primary requirement in today's communication world. These requirements are driven either by business need or by regulations. Many organizations find it difficult to derive a framework to define those requirements. In most cases, information has become the vital "asset" of businesses and is called "information asset" or "intellectual asset" [1]. It is essential to protect this asset so as to ensure its confidentiality, integrity, and availability [2]. While preserving these essential protections, the right information should be available to the right people, at the right place and at the right time. It is expected to make the information secure to guarantee that it is correct and available.

Also, it can be guaranteed that information is not jeopardized by misuse, which could lead to the loss of business and low performance of regulations. Obviously, information security management plays a very important and crucial role in each organization. The organization is expected to follow certain security compliance regulations and standards, together with the implementation of an information security management infrastructure. Therefore, an appropriate information security infrastructure, which is a vital need for most organizations, must be provided and implemented. Information security standards are helping organizations at this stage. There are many standards available for deriving a framework to define and structure the organization's requirements. As an example, one of the most applicable standards is ISO27001, which is an ISO accredited standard for information security management [2]. There are several reasons why an organization should implement the ISO27001 standard and the primary one will be the business demand [3].

Many organizations have introduced an ISMS to improve their security information management but always have big challenges to align goals of ISMS with their native security structure [4]. There are different ways of implementing an ISMS, but they are unable to implement it effectively and cannot keep it continuously within the organization. In this paper, a framework is proposed to cover ISO27001 and ISO17799 in such a manner that roles for all of the personnel in the organization are defined and each role has been assigned to predefined tasks. Also, each role has a specific workflow which is also defined in the framework. On the other hand and contrary to the ISO27001 standard which uses a waterfall model of implementation, in this proposed framework we will explore incremental and iterative mechanisms to implement an ISMS. Also, while implementing the ISMS, the proposed framework can figure out the status of the executed sections that makes the implementation effective.

This paper is organized as follows: first, we discuss related work and several existing methods. The proposed model is illustrated in Section 3. In Section 4, experimental results are presented. Conclusion and future work will be discussed in Section 5.

## 2. Related Work

*2.1. Information Security Management System.* Information security means protecting information and information systems [5]. Protection concept refers to the unauthorized access, disruption or, etc. Usually, the attacker exploits security goals (CIA): data confidentiality ($C$), data integrity ($I$), and service availability ($A$) using vulnerabilities that are a flaw or weak point in system security procedure, design, or implementation. Data confidentiality ensures that any authorized user can have access to only certain resources such as "information in database," "system configuration," and "network topology" which are needed to be protected against inappropriate disclosures. Integrity verifies that any authorized user can modify resources in an acceptable manner. Availability means that the assets are always accessible by the authorized users. An information security management system consists of some policies concerned with information security management. ISO/IEC 27001 standard gives overview of information security management systems. The key point in implementing ISMS is that it must remain effective and efficient over time. Thus, ISO/IEC 27001 standard incorporates *Plan-Do-Check-Act* (PDCA) cycle to keep long-term effectiveness and efficiency and adopt information systems changes [2]. PDCA is an iterative four-step management method. Unfortunately, a problem still occurs in the implementation of ISMS with PDCA; all activities scheduled in the *Plan* phase are only performed later in the *Do* phase. ISMS implementation experiences in the past few years indicate that the proposed method has still not reached full maturity and could not ensure that ISMS remains effective and stable over time. Indeed, it emerged as a nonincremental method. The proposed algorithm not only keeps the iterative nature of the PDCA model but also manages all activities incrementally.

*2.2. Risk Assessment.* Risk assessment is a major part of the ISMS Process. There are two types of risk assessment: (1) online: online risk assessment is a real-time process of evaluation and provides a risk index related to the host or network. Online risk assessment is very important in terms of minimizing the performance cost incurred. In the dynamic model, we can dynamically evaluate attack cost by propagating the impact of confidentiality, integrity and availability through dependencies model or attack graph [6–12]. (2) Offline: in Information security management system we use offline risk assessment. The information security management system standards specify guidelines and a general framework for risk assessment. In many existing standards, such as NIST and ISO27001, risk assessment is described. However, while these standards present some guidelines, there are no details on how to implement it in an organization. In a complex organization, risk assessment is a complicated process which involves many assets.

Guan et al. [13] assessed information security risks according to the likelihood and impact factors of each. In this method, risk factors are determined according to standard ISO17799 categorization. Then, it is assumed that determining the likelihood of each risk is similar to determining the weights in pairwise comparisons in the AHP method. Based on this view, the likelihood or weight of each risk factor is being determined using experts' opinions. On the other hand, the vulnerability of each information asset for each risk factor is considered equal to its impact severity, which takes its relative value from experts through linguistic variables.

Wang and Elhag [14] proposed a fuzzy TOPSIS method based on alpha level sets and applied it in bridge risk assessment. In this example, the likelihood and impact of different threats are being determined in linguistic variable forms and then are applied in bridge risk assessment by multiplying their related fuzzy values. Likewise, four effective criteri on impact severity are introduced. Experts express their opinion in the form of these four criterion, with which the severity impact is then calculated.

Kondakci [15] presented a composite system used for quantitative network security assessment. The idea is preventing the evaluation of each asset separately by applying repetitive attacks. The proposed model (composite system) generates and executes attacks once, composes risk data, and uses the risk data for the entire network in order to perform the overall assessment.

We agree with the arguments presented in [15, 16] that existing risk assessment models are often difficult to implement and handle in real world contexts without using appropriate software, because of their computational complexity. We are interested as [15, 16] to offer a model that not only tries to represent risk effect with a quantitative value but also can be easily implemented by any organization in the SUP model. Another important point is that all of the steps of proposed risk assessment are managed in SUP structure incrementally and iteratively.

*2.3. Contribution.* The main contributions of this paper can be summarized as (1) contrary to the ISO27001 standard which uses a waterfall model of implementation, in this proposed framework we will explore incremental and iterative mechanisms to implement an information security management system. The iterative approach can prevent project failure and cause robust implementation of security goals in the last iteration. (2) Role segregation has not been considered in ISO27001 standard and other security models properly. SUP proposes an appropriate role segregation and makes sure that we establish a framework where we can easily segregate security roles, and responsibilities. Roles have been segregated into about 20 roles and in each phase of SUP, it is clear which activities have to be done by each role and which artifacts have to be generated. (3) Since the proposed model is incremental and iterative, one of the important features of SUP is monitoring. Monitoring ensures that we established a framework to monitor roles, responsibilities, new assets, security policies and continuity of the executive committee of the organization. (4) In SUP, we present the FEMRA (fuzzy expert model for risk assessment) model, which uses a fuzzy expert system for risk assessment in organizations. Many risk assessment models have been proposed during the last decade. The distinguishing feature that separates our model from previous models is that all the steps to assess risk are done incrementally and iteratively based on the SUP structure. (5) To determine the risk, effective criterions are considered, and experts present their opinion with respect to these criterions. It leads us to increased accuracy and reliability of the results. (6) Asset classification plays a very important role in information security management. In the proposed risk assessment, we have designed a security cube (an asset classification), which is a combination of the valuable and important assets of the organization from a security perspective.

## 3. Proposed Model

SUP is an iterative and incremental approach that can help design, implement, monitor, and manage information security management system. This approach provides any organization with a predictable life-cycle security process for the development, adoption, and continual improvement of the information security solution [17]. Several fundamental principles which support successful iterative development are laid at the core of the SUP and represent the essential structure of the SUP [18, 19].

(i) Classify the assets with the proposed security cube.

(ii) Identify high risks early and manage continuously.

(iii) Work as a team.

(iv) Improve quality of implementation over time.

(v) Implement a modular ISMS with components.

*3.1. Why Develop Iteratively and Incrementally?* In the waterfall method, the biggest problem is that risk management will be reduced whenever the business model, assets identification, threats, and/or vulnerabilities are not perfectly

known. Another problem of the waterfall method for the implementation of an ISMS is that the strategies of future phases are not considered before they are started. The initial idea behind developing an ISMS iteratively is that, in contrast with the waterfall implementation, the developer is allowed to take advantage of what was learned during the development of earlier, incremental, deliverable versions of security levels within the organization. Learning comes from both the development and reaching the security levels, where possible. Risks are mitigated earlier, because elements are integrated progressively. We can accommodate changing the requirements in this method. We can facilitate the ISMS improvement and refinement which results in more robust ISMS. An iterative approach is generally superior to a linear or waterfall approach for many different reasons [20].

In the security unified process, iterations are planned in number, duration, and objective. A proper assessment of objectives enables the move to the next iteration successfully. The iterative approach can prevent project failure and cause robust implementation of security goals in the last iteration.

*3.2. Structure of the SUP.* As seen in Figure 1, the proposed information security management model includes two dimensions: static, which are disciplines, and dynamic, which are phases. In this architecture, the static dimension comprises six disciplines that are represented by business modeling, asset, security policy, implementation, configuration and change management, and project management. The dynamic dimension contains four life-cycle phases that are illustrated by inception, analysis and design, construction, and monitoring. Also, each phase can iterate. The area under the curve that is associated with each discipline shows the relative amount of effort and activity required to perform it over time. Along the vertical axis are the disciplines, which are a collection of workflows related to a major *area* of concern within the overall project [17, 18]. Figure 2 presents asset discipline.

A workflow consists of some activities that produce a result of observable value. Figure 3 presents, identifies and analyzes risk workflow. As seen in Figure 3, in each workflow, we have some roles, activities, and artifacts that are integrated to provide the goal of workflow. Table 1 explains each concept of elements in workflows. As mentioned, role segregation has not been considered in ISO27001 standard and other security models properly. SUP proposes an appropriate role segregation and makes sure that we establish a framework where we can easily segregate security roles and responsibilities. As mentioned, Figure 3 illustrates one of the SUP model workflow, that are relevant to the asset discipline. Roles segregation is clearly shown in this workflow that includes eleven roles: *threat evaluator, network specialist, network security specialist, communication specialist, computer specialist, network designer specialist, vulnerabilities evaluator, software specialist, information security specialist, physical security specialist, and human resource analyzer.* Six activities have been specified, and in fact each role is responsible to perform the related subactivities. Also, all the artifacts (output of activities) should be updated, and each role has to keep updated the related sections of each artifact. Fifteen

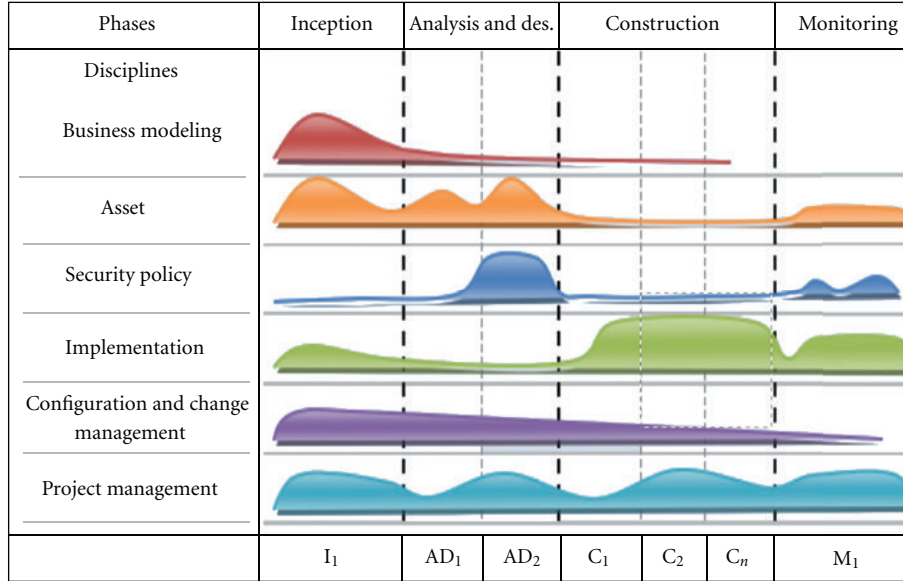| Phases | Inception | Analysis and des. | Construction | Monitoring |
|---|---|---|---|---|
| Disciplines | | | | |
| Business modeling | | | | |
| Asset | | | | |
| Security policy | | | | |
| Implementation | | | | |
| Configuration and change management | | | | |
| Project management | | | | |
| | $I_1$ | $AD_1$   $AD_2$ | $C_1$   $C_2$   $C_n$ | $M_1$ |

FIGURE 1: SUP architecture (phases: dynamic dimension; disciplines: static dimension).

artifacts are shown as the input artifacts that are generated in the previous workflows.

*3.3. Milestones.* From a security management perspective, all security life cycles of SUP are decomposed into four phases, and each phase is concluded by a major milestone. These milestones are represented by inception objectives, risk management, security level, and monitoring milestones. In each milestone, there are some major criteria that must be evaluated to determine whether the objectives of the phase have been met or not. These criteria are the phases objectives that must be reached. For instance, at the security-level milestone, the primary evaluation criteria for the construction phase involves the answers to these questions.

(i) Is the security level acceptable?

(ii) Are the identified risks reduced?

The construction phase may be started again if it fails to reach this milestone. A positive assessment shows that the project can be moved to the next phase successfully. Figure 4 shows the phases and milestones of a security management project at each phase end.

*3.4. Phases, Objectives, and Activities.* The inception phase is the first security project phase. In this phase, an accurate identification of the organization's business model as well as an asset identification is performed. The most important objectives in this phase that must be met and evaluated are.

(i) agreement that the cost/schedule estimates are appropriate.

(ii) agreement that the right set of security requirements have been obtained and that there is a common understanding of these requirements.

(iii) agreement that the identified assets are acceptable.

(iv) agreement that the defined risk assessment and management methodology is appropriate.

(v) formation of the executive committee of the organization.

Table 2 describes the activities during the inception phase of the SUP. During the analysis and Design phase, the analysis of assets to identify vulnerability points, threat points, and eventually risks is a vital step. During this phase, the most important objectives which need to be evaluated are as follows.

Activities of the Inception Phase

(i) Agreement that the classified assets are acceptable.

(ii) All risks have been identified, and a mitigation strategy exists for each.

(iii) Risks have been identified in accordance with the risk assessment and management methodology.

(iv) The designed system is in accordance with the identified risks.

(v) Agreement that the designed system reduces risks.

(vi) Writing the security policy.

Table 3 describes the activities of the analysis and design phase of the SUP. The construction phase focuses on implementing the designs resulting in risks reduction within an organization. Implementing the designs is based on a workflow that is extracted from the analysis and design phase. This workflow shows that a design can be started based on design priority. If we treat the base on design priority, the risks are reduced to an acceptable level. In SUP, security levels based on design priority are divided in five levels. On the other hand, the construction phase consists of five iterations. At the end of each iteration, the organization will reach a new security level. During this phase, the most important objectives that must be evaluated are as follows.
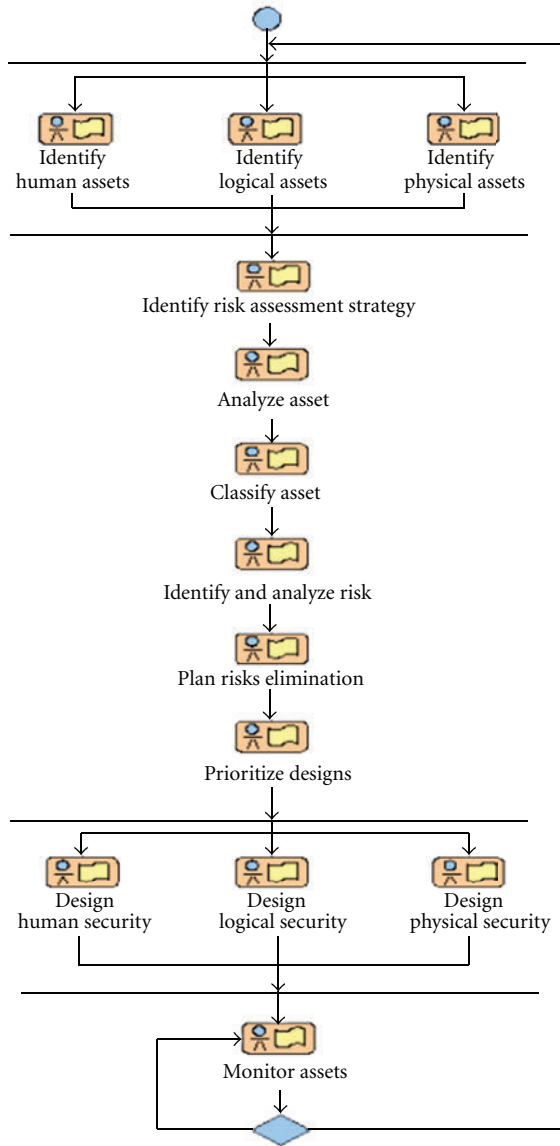
FIGURE 2: Asset discipline.

(i) Is the security level acceptable?

(ii) Are the identified risks reduced?

(iii) Agreement that the security level is acceptable.

Table 4 illustrates the activities of the SUP construction phase. During the monitoring phase, a monitoring program should be planned. The monitoring scope is the identification of new assets, vulnerabilities, and threats in asset discipline, reviewing the security policies in the security policy discipline and testing the implementations in the implementation discipline. The project manager must organize specific roles to ensure the ISMS effectiveness. During this phase, the most important objectives that must be evaluated are as follows.

(i) testing the implementation to keep the security at an acceptable level,

(ii) agreement that major risks do not exist.

Table 5 represents the activities of the SUP monitoring phase. ISO17799 includes eleven sections with 134 controls. Afterwards, ISO27001 has been developed as a wrapper to be put around ISO17799 to manage it with a PDCA model. By contrast, the SUP model comprises disciplines, workflows, and activities. Based on our structure, ISO17799 is mapped to the activities of the six disciplines and ISO27001 is mapped to the workflows of the six disciplines. Therefore, the percentage of project progress can easily be measured based on these two standards for each stage of the ISMS implementation project when using the SUP framework.

*3.5. Risk Assessment.* In SUP, we present the FEMRA (fuzzy expert model for risk assessment) model [21], which uses a fuzzy expert system for risk assessment in organizations. The risk assessment varies considerably with the context, the metrics used as dependent variables, and the opinions of the persons involved. Fuzzy logic thus represents an excellent model for this application. Organizations can use FEMRA as a tool to improve the ISMS implementation. One of the interesting characteristics of FEMRA is that it can represent each risk with a numerical value. The managers can detect higher risks by comparing these values and develop a good strategy to reduce them [22]. The relevant knowledge from human experts is stored as rule database in order to apply fuzzy logic and infer an overall numerical value [23]. There are three steps in the fuzzy model: fuzzification, inference engine, and defuzzification. The input and output of the fuzzy model is a number. In the inference engine, we define fuzzy rules. The first step in fuzzy logic processing involves a domain transformation called fuzzification. To transform crisp input into fuzzy input, membership functions must first be defined.

The next step is to apply if-then rules. The final step is defuzzification. This step is used to convert the fuzzy output set to a crisp number. We define three membership functions for input and output: low, medium, and high. Figure 5 illustrates the dependencies among some of the most important notions in the risk assessment terminology. There are three steps in the risk assessment model.

*Step 1.* The goal of the first step is to identify the assets and the potential threats applicable to the IT system. Three main bases of security known as the security golden triangle (confidentiality, integrity and availability) are used to evaluate assets, and calculate threat effects. Therefore, in this step, we have the CIA triad evaluated by experts.

*Step 2.* The goal of this step is to generate a list of asset vulnerabilities. We can then calculate asset values, vulnerability effects and threat effects.

*Step 3.* The goal of the final step is to calculate the risks. To calculate these effects, we use the fuzzy model that will be explained.

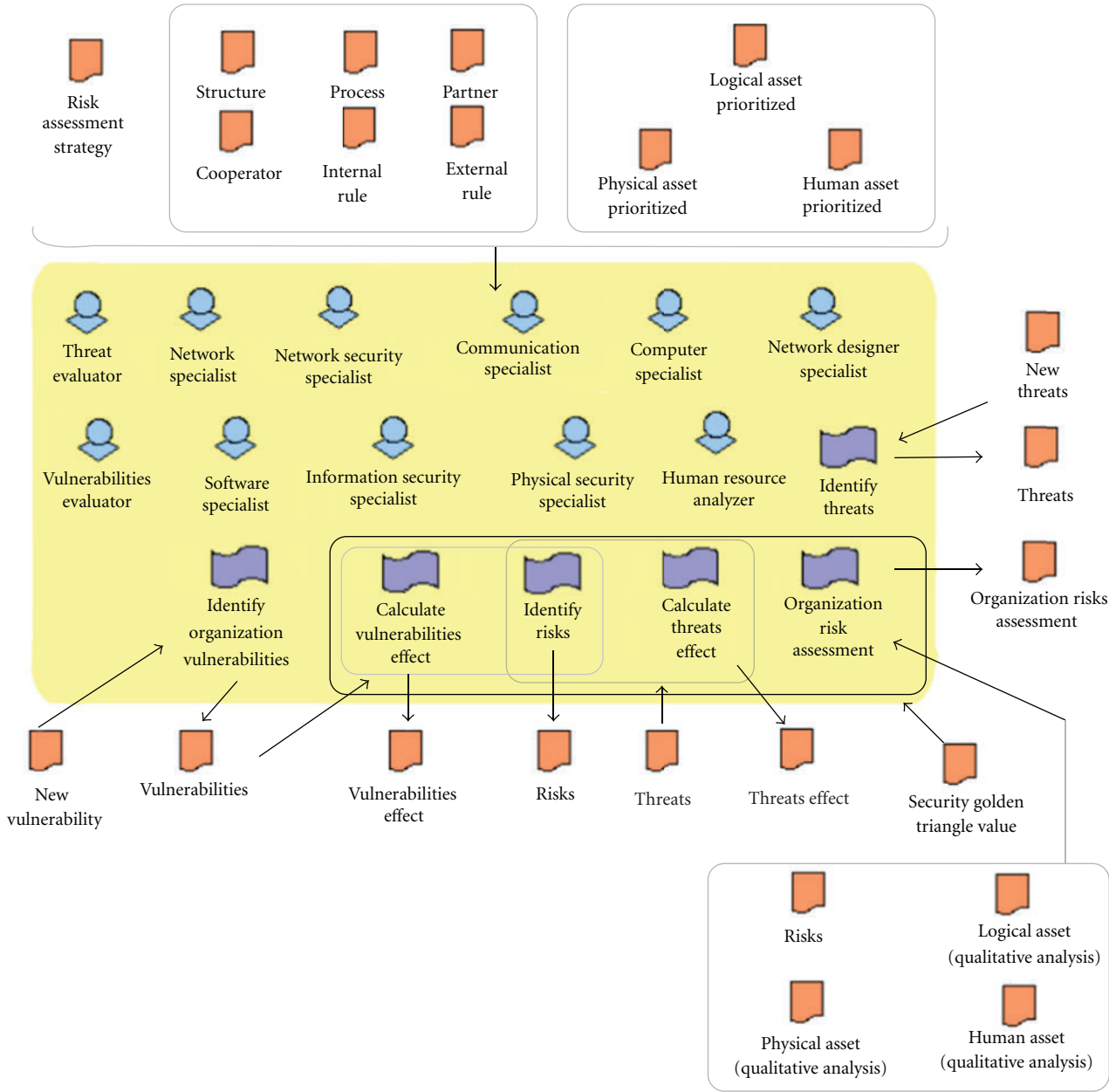Algorithm 1 illustrates the proposed risk assessment pseudocode.

FIGURE 3: Identify and analyze risk workflow.



FIGURE 4: The phases and milestones of SUP.

*3.5.1. Asset Classification and Identification.* Asset classification plays a very important role in information security management. So far, some methods have been proposed to classify the assets in organizations. If we can classify assets properly, it will help us achieve effective asset protection. In

the proposed asset classification, we have designed a security cube, which is a combination of the valuable and important assets of the organization from a security perspective, and the Zachman model [24]. Assets are classified according to three views.

(i) *Business View*. The business view consists of the three views of the Zachman framework (WHY-HOW-WHO), which includes value, policy, vision, mission, strategy, structure, process, partner, cooperator, internal rule, external rule, role, and human. There are also some empty fields that illustrate the flexibility of the model; some other parameters can be added to the cube.
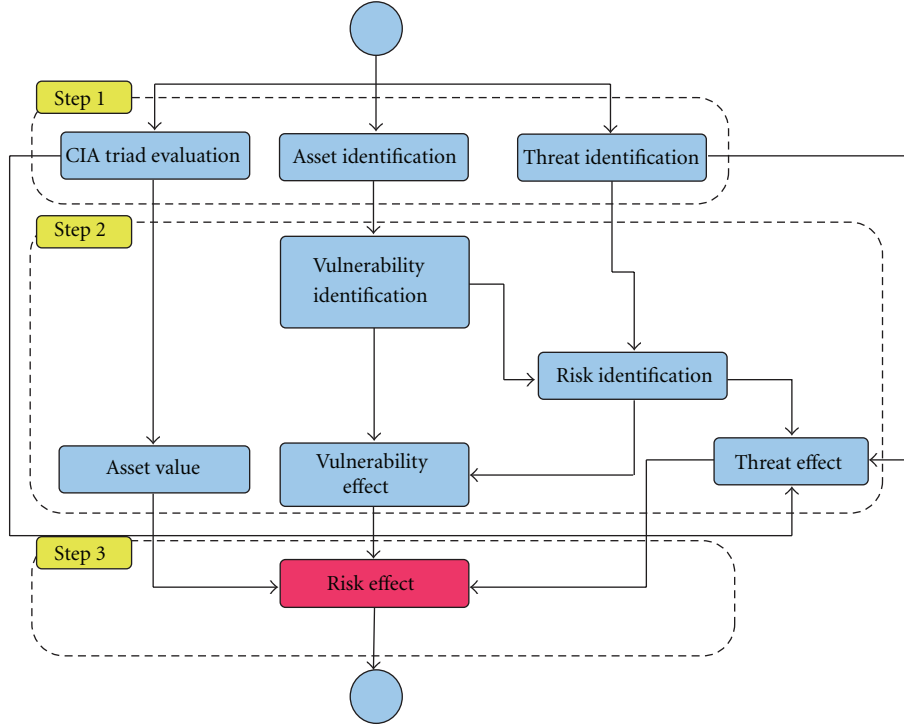
FIGURE 5: FEMRA risk assessment structure.

(ii) *Logical View.* The logical view is divided into three sections that are software, data, and logical infrastructure of networks. The data section is the WHAT view of the Zachman framework. The software section also is divided into foreign, country, and organization parts. Each part includes network tools, web application, application, programming, utility, DBMS, OS, and office. The data section is divided into personal and organizational parts, and each part comprises DB, file, paper, and brain storage. In the network section, the six parts are platform, application, strategy, protocol, communication, and design. Each part also includes different parameters that are illustrated in Figure 6.

(iii) *Physical View.* The physical view consists of four sections: media, storage, WHERE, and hardware components. The WHERE section is used as the WHERE view of the Zachman framework.

Each item in the cube should be evaluated with the four disciplines of SUP. This means that, when we are in the business modeling discipline, our view of each item is different than that from other disciplines. Additionally, in each discipline, each item should be evaluated with a *C-I-A* triad. Table 6 presents some examples of assets based on the security cube.

*3.5.2. Threat Identification.* A threat is something which may happen. When a threat materializes, it may result in

unwanted events which could damage the system or organization [2]. Threats can adversely affect assets. Table 7 shows some examples of threats.

*3.5.3. CIA Triad Evaluation.* Evaluating the *CIA* triad is key to calculate the organization's risks, and we can determine which one of these three complimentary goals is more important to an organization. The weight of confidentiality (*C*), integrity (*I*), and availability (*A*) are denoted as $w_C$, $w_I$, and $w_A$, respectively. We use $n$ experts (*e*) to evaluate the *CIA* triad. $\{C_e, I_e, A_e\} \in [0, 1]$. This illustrates the expert opinion in confidentiality, integrity, and availability respectively. Obviously, a higher number of experts would give a better risk assessment. Finally, the base of the *CIA* triad can be calculated with the following formula:

$$\{C_e, I_e, A_e\} \in [0, 1],$$
$$w_C = \frac{\sum_{e=1}^{n} C_e}{n},$$
$$w_I = \frac{\sum_{e=1}^{n} I_e}{n}, \tag{1}$$
$$w_A = \frac{\sum_{e=1}^{n} A_e}{n}.$$

Table 8 illustrates the opinion of $n$ experts about the *CIA* triad for a hypothetical organization.

*3.5.4. Vulnerability Identification.* A vulnerability is a flaw or weak point in system security procedures, design, or implementation. It could be exploited by an attacker or may

**Require:** SGT = [C, I, A] {Security-golden-triangle}
**Require:** E = [e₁, e₂, e₃,..., eₙ] {Experts}

  1: Cube = [Business, Logical, Physical] {Security Cube}
  2: Business = [Human]
  3: Logical = [Foreign, Country, Organization, Personal, Organizational, Platform, Application, Strategy, Protocol, Communication, Design]
  4: Physical = [Media, Storage, Where, Hardware Component]
  5: **for** each $d \in$ Cube **do**
  6:    **for** each $s \in d$ **do**
  7:      A = AssetIdentification($d, s$) {$d$: domains, $s$: sections}
  8:    **end for**
  9: **end for**
10: $T$ = ThreatIdentification() {Threat Identification $T = [t_1, t_1,..., t_n]$}
11: Evaluation($E$, SGT) {*CIA* Triad Evaluation}
12: **for** each $a \in A$ **do**
13:    $V[a]$ = VulnerabilityIdentification($a$) {Vulnerability Identification $V = [v_1, v_2..., v_n]$}
14: **end for**
15: $R$ = RiskIdentification($A$, $V$) {Risk Identification $R = [r_1, r_2,..., r_n]$}
16: **for** each $a \in A$ **do**
17:    AV[$a$] = AssetValue($E, a$) {Asset value}
18: **end for**
19: **for** each $v \in V$ **do**
20:    VE[$v$] = VulnerabilityEffect($E, v$) {Vulnerability Effect}
21: **end for**
22: **for** each $t \in T$ **do**
23:    TE[$t$] = ThreatEffect($E, t$) {Threat Effect}
24: **end for**
25: **for** each $r \in R$ **do**
26:    FRA = Fuzzification($r \cdot a$) {related asset}
27:    FRV = Fuzzification($r \cdot v$) {related vulnerability}
28:    FRT = Fuzzification($r \cdot t$) {related threat}
29:    RE[$r$] = defuzzification(FRA, FRV, FRT)
30: **end for**
31: **Return** SRE = Sort(RE)

ALGORITHM 1: Risk assessment ().

TABLE 1: Workflow elements.

| Symbol | Name | Description |
|---|---|---|
|  | Role | A role describes the responsibilities of person or a team in SUP. Role uses artifacts to perform activities and also generates some artifacts. |
|  | Activity | Activity identifies the work that roles do to obtain meaningful results. Activity has input and output artifacts. |
|  | Artifact | Artifact is a either final or intermediate product that is generated during the project. Artifact may be: (1) A document such as list of threats or vulnerabilities. (2) A model such as Risk Assessment Strategy |

affect the security goals of the *CIA* triad. Vulnerability identification can be achieved by different means such as software tools in networks, questionnaire forms, and so forth [23]. Table 9 presents some examples of asset vulnerabilities.

*3.5.5. Risk Identification.* The objective of risk identification is to identify all possible risks to the assets. In the previous sections, we exposed all the vulnerabilities of each asset. We also exposed all threats to the organization's assets. In this

Table 2: Activities of the inception phase.

| Discipline | Workflow | Activity |
|---|---|---|
| Business Modeling | Assess Business Status | Identify Organization Security Vision-Identify Organization Security Mission-Identify Organization Security Strategy-Identify Organization Security Policy-Identify Organization Security Value |
| | Identify Business Processes | Identify Business Structure-Identify Business Process-Identify Internal Rule-Identify External Rule-Identify Partner-Identify Cooperator |
| | Identify Roles and Responsibilities | Identify Human-Identify Role |
| Asset | Identify Human Asset | Identify Human |
| | Identify Logical Asset | Identify Organization Data-Identify Personal Data-Identify Organization Software-Identify Country Software-Identify Foreign Software-Identify Platform-Identify Network Services-Identify Network Design-Identify Protocol-Identify Communication Services |
| | Identify Physical Asset | Identify Media-Identify Storages-Identify Organization Map and Position-Identify Organization Hardware Components (Printer, Scanner, Fax, Modem, Antenna, Receiver, Sender, Camera, Fire Control, Access Control, Server Room, Server, Earthing Hole, Manhole, Duct, Riser, UPS, Mobile Computer, PC, USB, CD/DVD Writer, CD/DVD Reader, Flash Reader, FDD, Firewall, IDS, Switch, Router,…) |
| Security Policy | Indicate team members | Establish Management Team |
| Implementation | Indicate Scope of Implementation | Indicate Scope of Implementation |
| | Indicate Team Members | Establish Management Team-Establish Executive Team-Establish Advisor team |
| | Indicate Security Tools | Identify Organization Current Tools-Identify Security Tools-Identify Permitted tools-Indicate Buy Requirements |
| Configuration and Change Management | Plan Project Configuration and Change Control | Establish Configuration Management Policies-Establish Change Control Process |
| | Create Project Configuration Management Environment | Set up Configuration Management Environment |
| Project Management | Conceive New Project | Initiate Project-Develop Business Case-Identify and Assess Project Risks |
| | Create Security Plan | Define Project Organization and Staffing-Define Monitoring and Control Processes-Plan Phases and Iterations-Make Security Development Plan |
| | Monitor and Control Project | Monitor Project Status-Schedule and Assign Work-Report Status-Handle Exceptions and Problems |
| | Manage Iteration | Acquire Staff-Initiate Iteration-Assess Iteration |
| | Evaluate Project Scope and Risk | Identify and Assess Risks-Develop Business Case |
| | Close-Out Phase | Prepare for Phase Close-Out |
| | Plan for Next Iteration | Develop Iteration Plan-Develop Business Case |

TABLE 3: Activities of the analysis and design phase.

| Discipline | Workflow | Activity |
|---|---|---|
| Asset | Identify Risk Assessment Strategy | Identify Risk Assessment Strategy |
| | Analyze Asset | Identify Asset Lifecycle-Identify Asset condition-Identify Asset Qualitative Analysis-Acceptable Use of Asset-Give Value to the Security Golden Triangle |
| | Classify Asset | Label Asset-Prioritize Asset |
| | Identify And Analyze Risk | Identify Threats-Identify Organization Vulnerabilities-Calculate Vulnerabilities Effect-Calculate Threats Effect-Identify Risks-Organization Risks Assessment |
| | Plan Risks Elimination | Assign Risks to Designs |
| | Prioritize Designs | Identify Organization Security Levels-Prioritize Designs into Security Levels |
| | Design Human Security | Design Training Program-Segregation Security Role-Design Human events Procedure |
| | Design Physical Security | Design Earthing Hole-Design Physical Access Control-Design Fire Control-Design UPS-Design Camera-Design Wireless-Design Hardware Security Tools-Design Cabling-Design 2 and 3 Layer Tools-Design Server Room-Design Server Side-Design Client Side |
| | Design Logical Security | Design Availability-Design Reliability-Design Redundancy-Design Software Security Tools-Design Network Topology-Design Backup-Design Protocol-Design Switching-Design Logical Access Control-Design Zoning-Design Naming-Design Domain-Design Network Services-Design Platform-Design Communication Services-Design Software Framework Security-Design Source Security |
| Security Policy | Document Human Information Security Policy | Human Access Control Procedure-Human events Procedure-Training Program Procedure-Security Use of Data Procedure-Human Confidentiality Agreement Procedure-Exchange Agreement Procedure-Prior Employment Procedure-During Employment Procedure-Termination Employment Procedure-punishes Employment Procedure-Probable Events Procedure |
| | Document Logical Information Security Policy | Policy Cryptographic Procedure-Regulation Cryptographic Procedure-Information Handling Procedure-Data Exchange Procedure-Logical events Procedure-Logical Asset removal procedure-Logical Separation of Development Procedure-Logical Disposal and Reuse Procedure-User Registration Procedure-Mobile Computing-Teleworking-Monitoring System Procedure-Input Validation Procedure-Output Validation Procedure-Control Internal Processing Procedure-Restriction Change Package Procedure-Control Installation Package Procedure-Sensitive System Isolation Procedure-Out Sourcing Procedure-Internal Producing Procedure-Availability Procedure-Reliability Procedure-Redundancy Procedure-Software Security Tools Procedure-Network Topology Procedure-Backup Procedure-Protocol Procedure-Switching Procedure-Logical Access Control Procedure-Zoning Procedure-Naming Procedure-Domain Procedure-Network Services Procedure-Platform Procedure-Communication Services Procedure-Software Framework Security Procedure-Source Security Procedure |

TABLE 3: Continued.

| Discipline | Workflow | Activity |
|---|---|---|
| | Document physical Information Security Policy | Physical Asset Removal Procedure-Physical Separation of Development Procedure-Sitting and Protection Procedure-Supporting Utilities Procedure-Equipment Maintenance Procedure-Clean Environment procedure-mobile computer procedure-Physical Disposal and Reuse Procedure-Human events Procedure-Earthing Hole procedure-Physical Access Control procedure-Fire Control procedure-UPS procedure-Camera procedure-Wireless procedure-Hardware Security Tools procedure-Cabling procedure-2 and 3 Layer Tools procedure-Server Room procedure-Server Side procedure-Client Side procedure |
| Implementation | Buy Security Tools | Prioritize Need Tools |
| Configuration and Change Management | Manage Change Requests | Submit Change Request-Update Change Request-Review Change Request-Confirm Duplicate or Rejected CR |
| Project Management | Monitor and Control Project | Monitor Project Status-Schedule and Assign Work-Report Status-Handle Exceptions and Problems |
| | Manage Iteration | Acquire Staff-Initiate Iteration-Assess Iteration |
| | Evaluate Project Scope and Risk | Identify and Assess Risks-Develop Business Case |
| | Close-Out Phase | Prepare for Phase Close-Out |
| | Plan for Next Iteration | Develop Iteration Plan-Develop Business Case |

TABLE 4: Activities of the construction phase.

| Discipline | Workflow | Activity |
|---|---|---|
| Implementation | Implement Physical Design | Prioritize Physical Design-Schedule Physical Design-Implement Earthing Hole-Implement Physical Access Control-Implement Fire Control-Implement UPS-Implement Camera-Implement Wireless-Implement Hardware Security Tools-Implement Cabling-Implement 2 and 3 Layer Tools-Implement Server Room-Implement Server Side-Implement Client Side |
| | Implement Logical Design | Prioritize Logical Design-Schedule Logical Design-Implement Availability-Implement Reliability-Implement Redundancy-Implement Software Security Tools-Implement Network Topology-Implement Backup-Implement Protocol-Implement Switching-Implement Logical Access Control-Implement Zoning-Implement Naming-Implement Domain-Implement Network Services-Implement Platform-Implement Communication Services-Implement Software Framework Security-Implement Source Security |
| | Implement Human Design | Prioritize Human Design-Schedule Human Design-Implement Training Program-Implement Human events Procedure |
| Configuration and Change Management | Manage Change Requests | Submit Change Request-Update Change Request-Review Change Request-Confirm Duplicate or Rejected CR |
| Project Management | Monitor and Control Project | Monitor Project Status-Schedule and Assign Work-Report Status-Handle Exceptions and Problems |
| | Manage Iteration | Acquire Staff-Initiate Iteration-Assess Iteration |
| | Evaluate Project Scope and Risk | Identify and Assess Risks-Develop Business Case |
| | CloseOut Phase | Prepare for Phase Close-Out |
| | Plan for Next Iteration | Develop Iteration Plan-Develop Business Case |

TABLE 5: Activities of the monitoring phase.

| Discipline | Workflow | Activity |
| --- | --- | --- |
| Asset | Monitor Asset | Identify New Asset-Identify New Treats-Identify New Vulnerabilities |
| Security Policy | Review Human Information Security Policy | Review All Procedure (monthly-seasonally-semesterly-yearly) |
| | Review Logical Information Security Policy | Review All Procedure (monthly-seasonally-semesterly-yearly) |
| | Review physical Information Security Policy | Review All Procedure (monthly-seasonally-semesterly-yearly) |
| Implementation | Monitor Physical Implementation | Test Earthing Hole-Test Physical Access Control-Test Fire Control-Test UPS-Test Camera-Test Wireless-Test Hardware Security Tools-Test Cabling-Test 2 and 3 Layer Tools-Test Server Room-Test Server Side-Test Client Side |
| | Monitor Logical Implementation | Test Availability-Test Reliability-Test Redundancy-Test Software Security Tools-Test Network Topology-Test Backup-Test Protocol-Test Switching-Test Logical Access Control-Test Zoning-Test Naming-Test Domain-Test Network Services-Test Platform-Test Communication Services-Test Software Framework Security-Test Source Security |
| | Monitor Human Implementation | Test Training Program-Test Human events Procedure |
| | Report Physical Implementation Monitoring | Report All Monitoring (monthly-seasonally-semesterly-yearly) |
| | Report Logical Implementation Monitoring | Report All Monitoring (monthly-seasonally-semesterly-yearly) |
| | Report Human Implementation Monitoring | Report All Monitoring (monthly-seasonally-semesterly-yearly) |
| Configuration and Change Management | Manage Change Requests | Submit Change Request-Update Change Request-Review Change Request-Confirm Duplicate or Rejected CR |
| Project Management | Monitor and Control Project | Monitor Project Status-Schedule and Assign Work-Report Status-Handle Exceptions and Problems |
| | Manage Iteration | Acquire Staff-Initiate Iteration-Assess Iteration |
| | Evaluate Project Scope and Risk | Identify and Assess Risks-Develop Business Case |
| | Close-Out Project | Prepare for Project Close-Out |
| | Plan for Next Iteration | Develop Iteration Plan-Develop Business Case |

Figure 6: SUP cube.

Table 6: Assets.

| ID | Domain | Section (sub) | Asset |
|---|---|---|---|
| A1 | Business view | Who (human) | John Smith |
| A2 | Logical view (software) | Organizational (app.) | Human Resource Application |
| A3 | Logical View (Data) | Organizational (DB) | SQL_Server_1 |
| A4 | Logical view (network) | Application (DNS) | DNS_1 |
| A5 | Logical view (network) | Design (VLAN) | VLAN_1 |
| A6 | Physical view | Hardware component (server room) | Server_Room_1 |

TABLE 7: Threats.

| ID | Threat |
|---|---|
| T1 | Cache poisoning attacks |
| T2 | Data deletion |
| T3 | SQL injection |
| T4 | VLAN hopping attacks |
| T5 | Earthquake |
| T6 | Data theft |
| T7 | Directory traversal |
| T8 | Data discovery |
| T9 | Physical theft |

TABLE 8: CIA triad evaluation.

| Expert | Confidentiality ($C$) | Integrity ($I$) | Availability ($A$) |
|---|---|---|---|
| $E_1$ | $c_1$ | $i_1$ | $a_1$ |
| $E_2$ | $c_2$ | $i_2$ | $a_2$ |
| $E_3$ | $c_3$ | $i_3$ | $a_3$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $E_n$ | $c_n$ | $i_n$ | $a_n$ |
| Weight | $w_C$ | $w_I$ | $w_A$ |

section, we determine which threats are related to which vulnerability. The relationship between each vulnerability and threat is a risk. Table 10 illustrates some risks within an organization.

*3.5.6. Asset Value (AV).* The *CIA* triad should be used to calculate the value of each asset. We use $n$ experts to evaluate each asset. To get better results, we should get help from different experts for each group of assets in the security cube. For example, network experts should evaluate network assets such as servers, clients, and firewalls, software experts should evaluate software assets such as web applications. Each expert assigns a value from one to nine to each part of *CIA* triad based on Table 12. For example, a value of nine for confidentiality means that this asset's privacy is very high and a value of one for availability means that the availability of the asset is not important. Finally, the asset's value could be calculated with formula (2). $AV_C$, $AV_I$, and $AV_A$ illustrates the calculation of asset value in confidentiality, integrity, and availability, respectively. Table 11 shows the calculation of asset value by $n$ experts:

$$\{C_e, I_e, A_e\} \in [1, 9],$$

$$AV_C = w_C \cdot \left( \frac{\sum_{e=1}^{n} C_e}{n} \right),$$

$$AV_I = w_I \cdot \left( \frac{\sum_{e=1}^{n} I_e}{n} \right),$$

$$AV_A = w_A \cdot \left( \frac{\sum_{e=1}^{n} A_e}{n} \right),$$

$$AV = AV_C + AV_I + AV_A. \tag{2}$$

*3.5.7. Vulnerability Effect (VE).* We represent vulnerability effects with a percentage, and, for better accuracy, we get help from $n$ experts. For example, 90% means a very high vulnerability percentage, which means that all threats related to this vulnerability have a high probability of occurring. Finally, the vulnerability effect could be calculated with formula (3). Table 13 shows experts' opinions for a given vulnerability

$$VE = \frac{\sum_{e=1}^{n} effect}{n}. \tag{3}$$

*3.5.8. Threat Effect (TE).* We used the *CIA* triad to calculate threat effects. We use $n$ experts to calculate those effects. For each threat, we should get help from relevant experts to get better results. The calculation method of threats is similar to the one for assets. Each expert assigns a value from one to nine to each part of the *CIA* triad based on Table 11. For example, a value of nine in confidentiality means that this threat in the confidentiality area is very dangerous. Similarly, the value one in availability means that this threat cannot be dangerous for the availability. Finally, the threat effects could be calculated with formula (4). $TE_C$, $TE_I$, and $TE_A$ illustrates the calculation of threat effect in confidentiality, integrity, and availability, respectively. Table 14 shows the calculation of threat effect by $n$ experts:

$$\{C_e, I_e, A_e\} \in [1, 9],$$

$$TE_C = w_C \cdot \left( \frac{\sum_{e=1}^{n} C_e}{n} \right),$$

$$TE_I = w_I \cdot \left( \frac{\sum_{e=1}^{n} I_e}{n} \right), \tag{4}$$

$$TE_A = w_A \cdot \left( \frac{\sum_{e=1}^{n} A_e}{n} \right),$$

$$TE = TE_C + TE_I + TE_A.$$

*3.5.9. Risk Effect (RE).* Risk effects are modeled using three parameters: asset values, vulnerability effects, and threat effects. The following subsections will show how the risk effect can be calculated with the fuzzy model:

$$AV \in [1, 9],$$

$$VE \in [1, 100],$$

$$TE \in [1, 9], \tag{5}$$

$$RE = defuzz \cdot (fuzz \cdot (AV), fuzz \cdot (VE), fuzz \cdot (TE)).$$

TABLE 9: Asset vulnerabilities.

| ID | Asset | Vulnerability |
|---|---|---|
| V1 | A1 (John Smith) | No knowledge of file encoding using public keys |
| V2 | A2 (Human Resource Application) | Unchecked user input |
| V3 | A3 (SQL_Server_1) | Not using a mixed authentication mode |
| V4 | A4 (DNS_1) | Insufficient transaction ID space |
| V5 | A5 (VLAN_1) | Not properly configured |
| V6 | A6 (Serve_Room_1) | Unsuitable location |

TABLE 10: Some risks in an organization.

| Asset ID | Vulnerability ID | Threat ID | Risk ID |
|---|---|---|---|
| A1 | V1 | T9 | R1 |
| A2 | V2 | T3 | R2 |
| A2 | V2 | T7 | R3 |
| A3 | V3 | T2 | R4 |
| A3 | V3 | T6 | R5 |
| A3 | V3 | T8 | R6 |
| A4 | V4 | T1 | R7 |
| A5 | V5 | T4 | R8 |
| A6 | V6 | T5 | R9 |
| A6 | V6 | T9 | R10 |

TABLE 13: Vulnerability Effect.

| Expert | Effect |
|---|---|
| $E_1$ | $P_1\%$ |
| $E_2$ | $P_2\%$ |
| $E_3$ | $P_3\%$ |
| $\vdots$ | $\vdots$ |
| $E_n$ | $P_n\%$ |
| Effect | VE |

TABLE 14: Threat effect.

| Expert | Confidentiality ($C$) | Integrity ($I$) | Availability ($A$) |
|---|---|---|---|
| $E_1$ | $c_1$ | $i_1$ | $a_1$ |
| $E_2$ | $c_2$ | $i_2$ | $a_2$ |
| $E_3$ | $c_3$ | $i_3$ | $a_3$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $E_n$ | $c_n$ | $i_n$ | $a_n$ |
| Effect | $TE_C$ | $TE_I$ | $TE_A$ |

TABLE 11: Asset value.

| Expert | Confidentiality ($C$) | Integrity ($I$) | Availability ($A$) |
|---|---|---|---|
| $E_1$ | $c_1$ | $i_1$ | $a_1$ |
| $E_2$ | $c_2$ | $i_2$ | $a_2$ |
| $E_3$ | $c_3$ | $i_3$ | $a_3$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $E_n$ | $c_n$ | $i_n$ | $a_n$ |
| Value | $AV_C$ | $AV_I$ | $AV_A$ |

TABLE 12: Range.

| Level | Level | Effect |
|---|---|---|
| High | High | 9 |
| High | Medium | 8 |
| High | Low | 7 |
| Medium | High | 6 |
| Medium | Medium | 5 |
| Medium | Low | 4 |
| Low | High | 3 |
| Low | Medium | 2 |
| Low | Low | 1 |

(i) *Fuzzification*. Three membership functions are used for the three inputs, as can be seen in Figures 7(a), 7(b), and 7(c).

(ii) *Inference Engine*. The inference engine is fuzzy rule-based and is used to map an input space to an output space. The required rules for risk assessment are created as:

> **Rule 1:**
> *if (Threat_Effect = Low)*
> *then Risk_Effect = Low*
> **Rule 2:**
> *if (Threat_Effect = Medium and Vulnerability_Effect = Low)*
> *then Risk_Effect = Low*
> **Rule 3:**
> *if (Threat_Effect = Medium and Vulnerability_Effect = Medium)*
> *then Risk_Effect = Low*
> **Rule 4:**
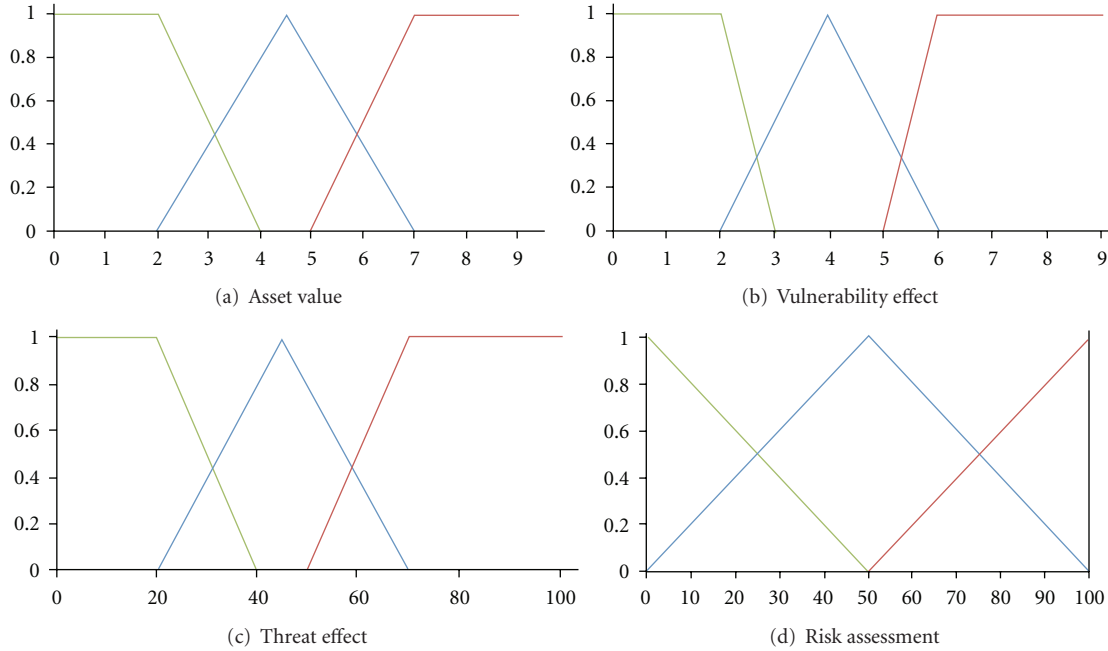> *if (Threat_Effect = Medium and Vulnerability_Effect = High)*

FIGURE 7: Three-level membership function.

(a) Asset value

(b) Vulnerability effect

(c) Threat effect

(d) Risk assessment

then Risk_Effect = Medium

**Rule 5:**

if (Threat_Effect = High and Asset_Value = Low)

then Risk_Effect = Medium

**Rule 6:**

if (Threat_Effect = High and Vulnerability_Effect = Low and

Asset_Value = Medium)

then Risk_Effect = Medium

**Rule 7:**

if (Threat_Effect = High and Vulnerability_Effect = Medium and

Asset_Value = Medium)

then Risk_Effect = Medium

**Rule 8:**

if (Threat_Effect = High and Vulnerability_Effect = High and Asset_Value = Medium)

then Risk_Effect = High

**Rule 9:**

if (Threat_Effect = High and Vulnerability_Effect = Low and Asset_Value = High)

then Risk_Effect = Medium

**Rule 10:**

if (Threat_Effect = High and Vulnerability_Effect = Medium and Asset_Value = High)

then Risk_Effect = High

**Rule 11:**

if (Threat_Effect = High and Vulnerability_Effect = High and Asset_Value = High)

then Risk_Effect = High

(iii) *Defuzzification.* Finally, we build another membership function to represent the different possibilities identified by the risk assessment, as displayed in Figure 7(d). This process is called defuzzification. Two of the most common techniques are the centroid method and maximum method. In the centroid method, the crisp value of the output variable is computed by finding the center of gravity of the membership function. In the maximum method, the crisp value of the output variable is the maximum truth value (membership weight) of the fuzzy subset. The defuzzification technique that is used for this model is the centroid method.

## 4. Results

*4.1. Risk Assessment.* Table 15 shows the results of the risk assessment method for some risks (which were extracted based on Table 10). In this table, the asset values, vulnerability effects, and threat effects were calculated with formulas (2), (3) and (4) and the risk effects were calculated based on these three previous values and the fuzzy model.

*4.2. SUP Framework.* To verify the efficiency of the proposed model, it has been implemented in two industrial organizations. They both had implemented ISMS based on ISO27001 three years ago but lost its continuity after seven months. The goal was to reimplement ISMS in these organizations but using the SUP method instead. After waiting seven months, it was possible to make a meaningful comparison between the status of this implementation and the one they had

TABLE 15: Risk assessment results.

| Risk ID | Asset Value (0–9) | Vulnerability effect (0–100) | Threat effect (0–9) | Risk effect (0–100) |
|---------|-------------------|------------------------------|---------------------|---------------------|
| R1 | 6.92 | 91.66 | 6.92 | 83.6 |
| R2 | 9 | 46.66 | 7.56 | 83.6 |
| R3 | 9 | 46.66 | 4.8 | 18.3 |
| R4 | 9 | 50 | 3.08 | 18.8 |
| R5 | 9 | 50 | 5 | 19.2 |
| R6 | 9 | 60 | 5 | 45.6 |
| R7 | 5.44 | 63.33 | 5.48 | 57.1 |
| R8 | 5 | 73.33 | 2.68 | 46 |
| R9 | 9 | 80 | 2.92 | 49.7 |
| R10 | 9 | 80 | 6.92 | 83.7 |

TABLE 16: The comparison between the two methods.

| Index no. | Index name | Organization 1 | | Organization 2 | |
|-----------|------------|----------------|------|----------------|------|
| | | ISO 27001 | SUP | ISO 27001 | SUP |
| 1 | Monitoring | 27 | 81 | 36 | 63 |
| 2 | Maintenance and continuity | 15 | 61 | 18 | 71 |
| 3 | Reporting | 43 | 60 | 51 | 70 |
| 4 | Customer confidence | 50 | 82 | 60 | 73 |
| 5 | Risk assessment | 50 | 93 | 50 | 80 |
| 6 | Business continuity | 48 | 66 | 56 | 49 |
| 7 | Role segregation | 10 | 96 | 11 | 98 |
| 8 | Configuration and change management | 10 | 40 | 12 | 36 |
| | Results | %32 | %72 | %37 | %67 |

with ISO27001. The results of these two implementations are presented in Table 16. The comparison between the two methods is based on 8 parameters, which are the most important aspects of the ISMS implementation.

  (i) *Monitoring*. This aspect ensures that we established a framework to monitor roles, responsibilities, new assets, security policies and continuity of the executive committee of the organization.

 (ii) *Maintenance and Continuity*. This aspect ensures that our Information Security Management System will not lose its stability over time. Continuity is one of the biggest challenges that all security managers deal with, because we have to consider security in all business processes, and it needs perfect risk assessment and management over time.

(iii) *Reporting*. This aspect ensures that we established a framework for easy and continuous reporting.

 (iv) *Customer Confidence*. customers expect their information to be secure and private. If we implement a powerful ISMS mechanism, we can improve customer confidence. For this purpose, we have to determine some indicators.

  (v) *Risk Assessment*. This aspect makes sure that our risk assessment model identifies high risks and prioritizes them properly. Obviously, it helps us more accurately reduce risks in the risk management step. Also, it makes sure that we have good asset classification. As mentioned, asset classification plays a very important role in information security management. If we can classify assets properly, it will help us to achieve an effective asset protection.

 (vi) *Business Continuity*. It makes sure that our business continuity management process prevents business disruptions and security failures and ensure that essential operations are restored as quickly as possible [2].

(vii) *Role Segregation*. It makes sure that we establish a framework where we can easily segregate security roles and responsibilities. Proper segregation helps other aspects of the ISMS implementation.

(viii) *Configuration and Change Management*. This aspect ensures that adapting to change, controlling change, and effecting change are under control. In ISMS, we have many security documents or policies that are related to each other, and changing a document is a challenge.

Each value in the aspect columns indicates the average of the top managers' opinions that have been gathered (all values are rounded up). Results show that SUP improves the ISMS implementation. The most impressive part of the results was shown in maintenance and continuity, role segregation, and risk assessment, because there is rarely success without iterative and incremental mechanisms. Also, significant improvements in other parameters cannot be ignored.

## 5. Conclusion

ISO27001 is the best framework to implement and maintain an organization's security. The most important point in this standard is that external certification of ISO27001 does not mean that you are really secure; it only means that you are managing security in line with the standard. On the other hand, ISO27001 points out methods for risk assessment and choosing controls and policies, but it never addresses the relations between all these parts as a well-designed integrated structure for security specialists. The results obtained clearly demonstrate the benefits of implementing the SUP framework to implement an ISMS. SUP has effectively improved the ISO27001 implementation process. Using the SUP framework within an organization leads to a better and higher-quality ISMS implementation. Effective management, increased success of the ISMS implementation, and well-defined tasks for each person who has a role in the ISMS implementation are precisely identified. One of the most important parts to ensure an effective ISMS implementation is the classification of assets, for which the security cube is proposed in the SUP method. To bring the organization to a certain security level, an incremental and iterative process has been designed. Therefore, security levels are divided into N levels, and by achieving each one, the organization will reach the desired security. For each of these levels, or iteration, there is a workflow of designs. SUP have been implemented in two industrial organizations, and its results have been compared with the previous implementation status of ISMS. The results show the significant improvement in evaluation indicators.
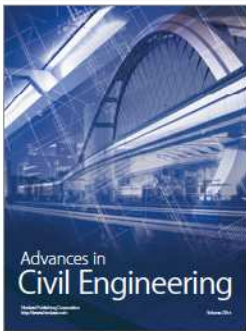
## References

[1] M. Dey, "Information security management—a practical approach," in *Proceedings of the IEEE AFRICON*, pp. 1–6, September 2007.

[2] ISO, "Information technology Security techniques Information security management systems Requirements," ISO/IEC 27001, 2005.

[3] J. Eloff and M. Eloff, "Information security management—a new paradigm," in *Proceedings of the SAICSIT*, pp. 130–136, 2003.

[4] J. S. Broderick, "ISMS, security standards and security regulations," *Information Security Technical Report*, vol. 11, no. 1, pp. 26–31, 2006.

[5] L. Chung, "Dealing with security requirements during the development of information systems," in *Proceedings of the 5th International Conference on Advanced Information Systems Engineering (CAiSE '93)*, pp. 234–251, Paris, France, 1993.

[6] S. Kondakci, "A new assessment and improvement model of risk propagation in information security," *International Journal of Information and Computer Security*, vol. 1, no. 3, pp. 341–366, 2007.

[7] S. Kondakci, "A causal model for information security risk assessment," in *Proceedings of the 6th International Conference on Information Assurance and Security*, pp. 143–148, IEEE Computer Society, 2010.

[8] S. Kondakci, "Network security risk assessment using bayesian belief networks," in *Proceedings of the 2nd IEEE International Conference on Social Computing, IEEE International Conference on Privacy, Security, Risk and Trust*, pp. 952–960, IEEE Computer Society, August 2010.

[9] S. Kondakci, "A recursive method for validating and improving network security solutions," in *Proceedings of the International Conference on Security of Information and Networks (SIN '07)*, pp. 74–83, Trafford Publishing, 2007.

[10] C. Pak, "The near real time statistical asset priority driven (NRTSAPD) risk assessment methodology," in *Proceedings of the 9th ACM SIG-Information Technology Education Conference (SIGITE '08)*, pp. 105–112, ACM, October 2008, New York, NY, USA.

[11] C. Pak and J. Cannady, "Asset priority risk assessment using hidden Markov models," in *Proceedings of the 10th ACM Special Interest Group for Information Technology Education (SIGITE '09)*, pp. 65–73, Fairfax, Va, USA, October 2009.

[12] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng, "A markov game theory-based risk assessment model for network information system," in *Proceedings of the International Conference on Computer Science and Software Engineering (CSSE '08)*, pp. 1057–1061, December 2008.

[13] B. C. Guan, C. C. Lo, P. Wang, and J. S. Hwang, "Evaluation of information security related risks of an organization—the application of the multi-criteria decision-making method," in *Proceedings of the 37th IEEE Annual International Carnahan Conference on Security Technology*, pp. 168–175, October 2003.

[14] Y. M. Wang and T. M. S. Elhag, "Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment," *Expert Systems with Applications*, vol. 31, no. 2, pp. 309–319, 2006.

[15] S. Kondakci, "A composite network security assessment," in *Proceedings of the 4th International Conference on Information Assurance and Security*, pp. 249–254, IEEE Computer Society, 2008.

[16] M. Hamdi and N. Boudriga, "Algebraic specification of network security risk management," in *Proceedings of the ACM Workshop on Formal Methods in Security Engineering (FMSE '03)*, pp. 52–60, October 2003.

[17] L. Muller, M. Magee, P. Marounek, and A. Philipson, "IBM IT governance approach-business performance through IT

execution," 2008, http://www.redbooks.ibm.com/abstracts/sg247517.html.

[18] IBM Rational Unified Process (RUP), http://www-01.ibm.com/software/awdtools/rup.

[19] P. Kroll and P. Kruchten, *Rational Unified Process Made Easy: A Practitioner's Guide to the RUP*, Addison-Wesley, Boston, Mass, USA, 2003.

[20] C. Larman and V. R. Basili, "Iterative and incremental development: a brief history," *Computer*, vol. 36, no. 6, pp. 47–56, 2003.

[21] A. Shameli-Sendi, M. Jabbarifar, M. Shajari, and M. Dagenais, "FEMRA: fuzzy expert model for risk assessment," in *Proceedings of the 5th International Conference on Internet Monitoring and Protection*, pp. 48–53, Barcelona, Spain, 2010.

[22] K. Haslum, A. Abraham, and S. Knapskog, "Fuzzy online risk assessment for distributed intrusion prediction and prevention systems," in *Proceedings of the 10th International Conference on Computer Modeling and Simulation*, pp. 216–223, IEEE Computer Society Press, Cambridge, UK, 2008.

[23] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[24] J. A. Zachman, "The Zachman framework," http://www.zachmaninternational.com/.

Journal of
Engineering

The Scientific
World Journal

International Journal of
**Rotating**
**Machinery**

Journal of
Sensors

International Journal of
Distributed
Sensor Networks

Advances in
Civil Engineering

Journal of
**Control Science**
**and Engineering**

Journal of
Robotics

**Hindawi**

Submit your manuscripts at
http://www.hindawi.com

Journal of
Electrical and Computer
Engineering

Advances in
OptoElectronics

**VLSI Design**

International Journal of
Navigation and
Observation

Modelling &
Simulation
in Engineering

International Journal of
**Aerospace**
**Engineering**

International Journal of
Chemical Engineering

International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components

Shock and Vibration

Advances in
Acoustics and Vibration