International Journal of Safety and Security Engineering
Vol. 13, No. 6, December, 2023, pp. 987-1000
Journal homepage: http://iieta.org/journals/ijsse

Roadmap and Information System to Implement Information Technology Risk Management

Hasnaa Berrada*, Jaouad Boutahar, Souhail El Ghazi El Houssaini

Systems Architectures and Networks Team in EHTP (Ecole Hassania des Travaux Publics - Hassania School of Public Works), Casablanca 8108, Morocco

Corresponding Author Email: berrada.hasnaa.cedoc@ehtp.ac.ma

https://doi.org/10.18280/ijsse.130602

Received: 22 October 2023
Revised: 5 December 2023
Accepted: 18 December 2023
Available online: 25 December 2023

Keywords:
IT risk management, COBIT 5, roadmap, information system, COSO ERM, IT risk deliveries, IT risk processes, ISO 31000

ABSTRACT

In the pursuit of strategic and economic goals, risk management has become indispensable for organizations. Information technologies hold a central position in organizational operations, necessitating adaptable information systems that can effectively navigate associated risks. While numerous standards and frameworks are dedicated to Enterprise Risk Management (ERM), Information Technology Risk Management (ITRM) is addressed less frequently. Within this domain, COBIT 5 emerges as a notable guide, offering audit and governance principles tailored to ITRM. Nevertheless, COBIT 5, alongside other benchmarks, is observed to lack comprehensive, structured guidelines that support an integrated approach. This paper introduces a proposed roadmap and its supporting information system, drawing upon the foundations laid by ISO 31000, COSO ERM, and COBIT 5. The roadmap is designed to address the dearth of detailed frameworks in ITRM, presenting a holistic strategy that elucidates and simplifies the sequential steps and expected deliverables. The principal aim is to provide a structured methodology for the implementation of ITRM in organizations. Looking to the future, the potential application of Artificial Intelligence (AI) to further automate and refine this approach represents an intriguing avenue for research and development. The roadmap thus sets the stage for a transformative leap in ITRM, promising enhanced efficacy and strategic alignment.

1. INTRODUCTION

The engagement with risk is a fundamental aspect of organizational strategy and operational execution, where its management is crucial for ensuring the attainment of successful outcomes [1-3]. This intersection of risk and strategic objectives has garnered significant attention in scholarly discourse and among industry professionals.

Concurrently, information technology (IT) and information systems (IS) have become integral to daily operations, enhancing efficiency and simplifying complex tasks [4]. The centrality of IT within organizational structures is undeniable, conferring a competitive edge and supporting virtually all facets of organizational functions [5]. The ubiquitous need for IT support is evident across the complete spectrum of daily activities within modern organizations [6]. However, this widespread integration of IT is not without its challenges. The accelerated adoption of information technologies has ushered in an era of elaborate and intricate risks. These risks, ever-expanding in scope and complexity, are frequently characterized as formidable. Organizations are thus compelled to confront IT risks, which have emerged as a critical focal point due to their potential impacts on both internal and external organizational dynamics [6].

In the contemporary corporate sphere, entities must navigate a landscape replete with a plethora of IT-related risks. These risks encompass a spectrum of issues such as cybersecurity threats, including malware, phishing, and insider attacks; data breaches and loss; system failures and associated downtime; risks stemming from third-party associations; challenges linked to the adoption of new technologies and innovation; physical security concerns; and the perennial threats of operational mishaps and human error [7]. The ramifications of insufficient or ineffective IT risk management can be profound. Notably, an outage of Amazon Web Services (AWS) in 2017 severely disrupted a multitude of online services and websites, serving as a stark reminder of the vulnerabilities associated with dependence on a solitary cloud service provider [8]. Furthermore, the extended grounding of Boeing's 737 Max aircraft, which was partially ascribed to software issues sourced from a third-party vendor, inflicted substantial financial losses on the company, estimated in the tens of billions of dollars [9-11]. Additionally, in 2012, the Knight Capital Group experienced a significant system malfunction that inadvertently triggered a volley of unplanned transactions, culminating in a financial blow of around $440 million and necessitating an acquisition to avert insolvency [12].

Within the dynamic and risk-laden environment of contemporary organizations, a comprehensive approach to Information Technology Risk Management (ITRM) is recognized as essential for safeguarding uninterrupted business operations from both external and internal IT threats [13].

Multiple standards related to ITRM are available, yet these often fall into two distinct categories: those that are generic and encompass Enterprise Risk Management, such as ISO 31000 [14], ISO Guide 73 [15], and COSO ERM [16], along with frameworks like the AMF [17]; and those that are specific to information security risk management, including ISO 27005 [18], ISO 27000 [19], and NIST CSF [7]. Among these, COBIT 5 [20] emerges as an IT audit and governance framework [21] that includes "COBIT 5 for Risk" [22], a publication specifically dedicated to ITRM. Nevertheless, the application of COBIT 5 within organizations is often met with challenges due to the absence of a structured and integrated method for ITRM deployment [23].

This research contributes to the field of ITRM by proposing an integrated approach and comprehensive system. Previously, in 2021, a methodological framework and system were detailed for auditing the maturity of ITRM practices within organizations [24]. Building on this foundation, the current article introduces a roadmap and corresponding system designed for the implementation of ITRM.

The manuscript is structured as follows: an initial overview of related literature to ITRM is provided. Subsequently, the methodological framework employed in crafting the roadmap is explicated. The third section is trifurcated, with the first part delineating the proposed roadmap for ITRM implementation, the second part detailing the UML design of the information system, and the third part showcasing screenshots of the actual system developed. The final section encapsulates the findings and implications of the study.

2. RELATED WORK

IT risk is defined as the "business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise" [22].

On the other hand, the Enterprise Risk Management (ERM) represents a holistic approach to manage risks faced by an organization, whether public or private, listed or unlisted [25].

Concerning ERM frameworks, many of them exist. For example, COSO, a recognized reference of internal control [16]. The version of 2017, COSO ERM (Enterprise Risk Management), a frame that proposes lines of thoughts covering the fields of strategy development and execution. However, the application of this updated version may require from organizations to develop a more precise in-house methodological framework defining the practical procedures for applying the concepts it contains [25].

Besides COSO ERM, there is the standard ISO 31000 that proposes principles and guidelines for Enterprise Risk Management [14]. It contains three chapters: principles, framework, process. "Geraldine Sutra" in her publication "Management du risque: une approche stratégique" stated that it is always a good idea for organizations to translate the content of ISO 31000 into their own internal methodological framework [25].

The COBIT framework was created by ISACA, the Information Systems Audit and Control Association can be considered as a framework that comprises IT risk management guidelines. COBIT stands for Control Objectives for Information and Related Technologies. It defines a set of processes for IT management and governance [26]. This framework includes dedicated documentation for IT risk management which is "COBIT 5 For Risk" [22].

When it comes to information security risk management frameworks, the international standard ISO 27005 was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This standard provides guidelines for information security risk management and draws a generic risk management method [18].

In conclusion as presented in Table 1, COSO ERM and ISO 31000 are generic frameworks (ERM frameworks) that deal with all types of risks of organizations. Whereas, ISO 27005 is a standard that is specific for information security risk management. Only COBIT 5 contains specific publication, "COBIT 5 for risk", for IT risk management.

In fact, COBIT5 can be used to implement IT risk management within organizations. However, its deployment is difficult for many reasons as stated below [27, 28]:

- A large cohort of publications on IT governance exists that can be used for IT risk management but requires simplification and structuring of the key concepts related to ITRM.
- A specific documentation for ITRM. However, it does not present an integrated, structured and simplified approach to implementing IT risk management in an organization.
- COBIT 5 includes 2 processes dedicated to risk management: APO12 (Manage risk) and EDM03 (Ensure risk optimization). However, we note the absence of a chronology of steps to follow for the successful deployment of IT risk management in an organization.

In the literature, some research articles used COBIT 5 for the implementation of IT risk management. Authors "Walid Al-Ahmad" and "Basil Mohammed" in their article [23] describe operational processes, sub-processes, activities and guidelines to use in order to implement information security risk management. In this article, only the process APO12-Manage Risks of COBIT 5 that was used. Thus, the process EDM03-Ensure Risk Optimization was not considered for that implementation. Besides, we note that the article focused on information security risk management only ignoring an integrated scope of IT risk management.

Astuti et al. [29] tried to deploy the two COBIT 5 processes DSS02 Manage service and APO12 Manage Risks on a case study of ITS service desk. The objective of the article was to identify, assess and manage risks related to Information Technology processes of service desk organizational unity. As the precedent article, the process EDM03-Ensure Risk Optimization was not used into the implementation.

Table 1. Comparison of risk management frameworks

Framework	ERM Framework	IT Risk Management Framework	Information Security Risk Management Framework
COSO ERM	✓	✗	✗
ISO 31000	✓	✗	✗
ISO/CEI 27005	✗	✗	✓
COBIT 5	✗	✓	✗

In the research article “Risk Assessment and Recommendation Strategy Based on COBIT 5 for Risk: Case Study SIKN JIKN Helpdesk Service” [30], the authors carried out a risk assessment of SIKN JIKN helpdesk activities, based on the COBIT 5 for risk, COBIT 5 Enabling process and COBIT 5 Framework guidelines. The approach adopted to carry out the case study was based mainly on the two processes DSS01 Manage operations and APO12 Manage risks. The method presented only covered the risk assessment stage, and therefore did not deploy the EDM03 Ensuring risk optimization, a risk governance process.

The main limitations identified in the various research articles cited above are as follows:

- Partial coverage of the implementation of an IT risk management system, focusing mainly on the risk identification and analysis phase, without considering the entire IT risk management and IT risk governance processes.
- Lack of an integrated end-to-end approach to IT risk management.

To respond to these limitations, our research work develops a simplified, integrated and global system for Information Technology Risk Management based on the combination of the three frameworks: ISO 31000, COSO ERM & COBIT 5.

3. METHODOLOGY

By combining three standards, we defined the roadmap that describes the phases and steps needed to implement Information Technology Risk Management. The methodological approach used ISO 31000 and COSO ERM to define the process and general concepts of Enterprise Risk Management and COBIT 5 to integrate the specific features of IT risk management:

- ISO 31000 (Version 2018): provides guidelines to manage all types of risks, and information technology risks in particular, and integrates them to this standard. Besides, ISO 31000 presents a process of risk management that begins with the establishment of the context and ends with the review and monitoring (Figure 1) [14].
- COSO ERM (Version 2017): is used as a generic framework that originally was not specific to IT and hence provides an approach to identify, assess, and manage risks of the whole organization, including information technology risks (Figure 2) [31].

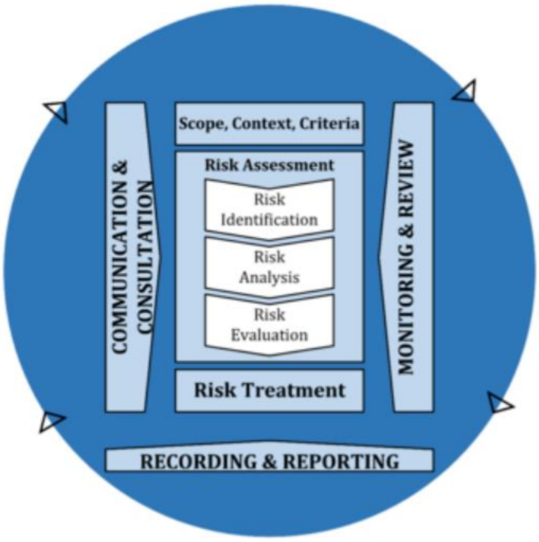


Figure 1. Risk management process, ISO 31000 [14]

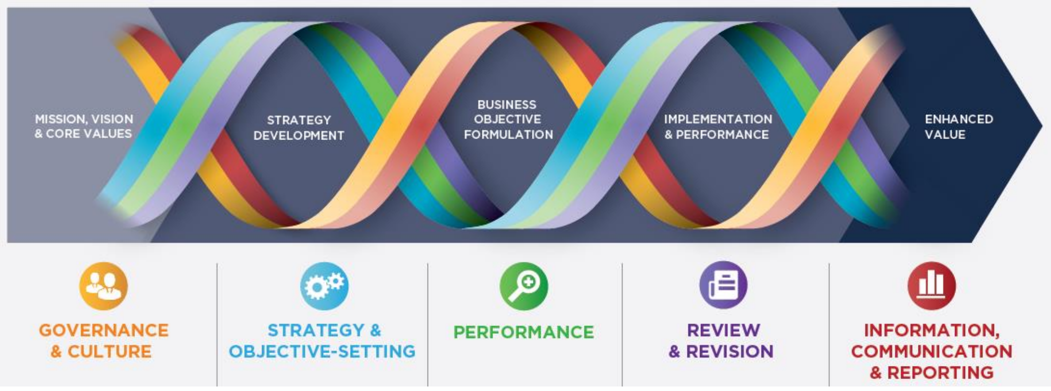
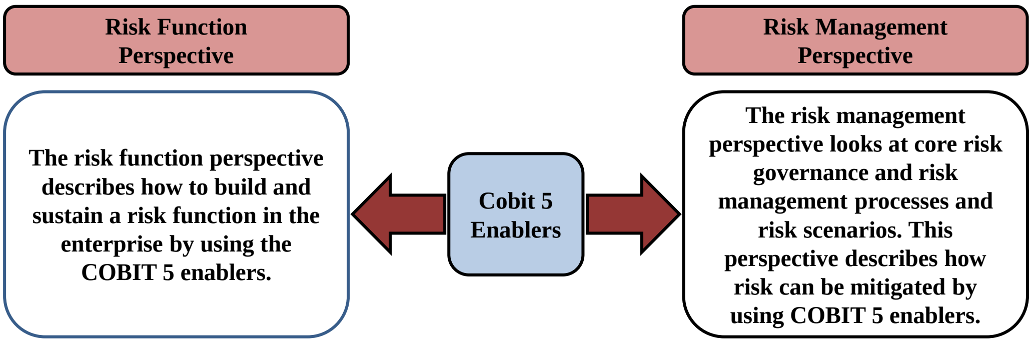

MISSION, VISION & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE
GOVERNANCE & CULTURE
STRATEGY & OBJECTIVE-SETTING
PERFORMANCE
REVIEW & REVISION
INFORMATION, COMMUNICATION & REPORTING

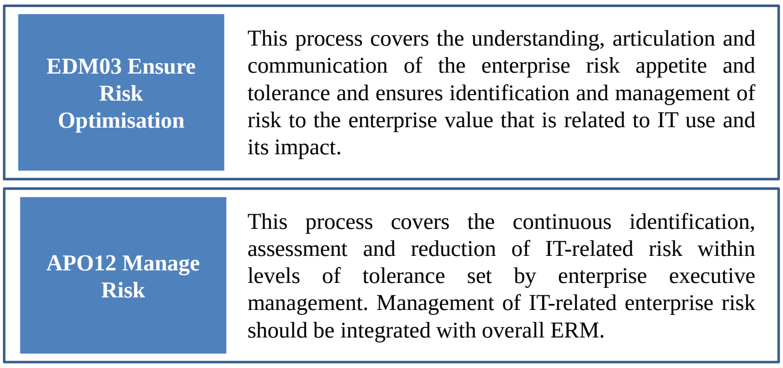
Figure 2. The 5 components of COSO ERM 2017 [31]



The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.

The risk management perspective looks at core risk governance and risk management processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

Figure 3. The two perspectives of risk proposed by COBIT 5 [22]



EDM03 Ensure Risk Optimisation

This process covers the understanding, articulation and communication of the enterprise risk appetite and tolerance and ensures identification and management of risk to the enterprise value that is related to IT use and its impact.

APO12 Manage Risk

This process covers the continuous identification, assessment and reduction of IT-related risk within levels of tolerance set by enterprise executive management. Management of IT-related enterprise risk should be integrated with overall ERM.

Figure 4. COBIT 5 core risk processes [22]

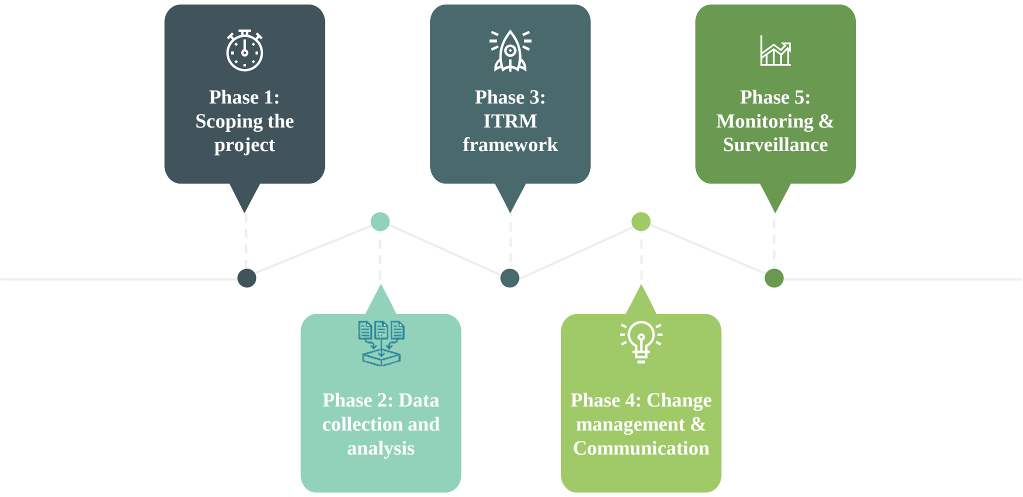

Phase 1: Scoping the project
Phase 3: ITRM framework
Phase 5: Monitoring & Surveillance
Phase 2: Data collection and analysis
Phase 4: Change management & Communication

Figure 5. A methodological approach to implement ITRM within organizations

Table 2. Development of the proposed approach by using ISO 31000, COSO ERM & COBIT 5

Proposed Approach	COSO ERM	ISO 31000	COBIT 5
Phase 1	Strategy & Objective-setting	Scope, context, Criteria	Not existent
Phase 2	Strategy & Objective-setting	Scope, context, Criteria	Manage risk (APO12)
Phase3	Performance	Risk Assessment Risk Treatment	Manage risk (APO12)
Phase 4	- Governance & Culture - Information, Communication & Reporting	- Recording and Reporting - Communication & Consultation	- Ensure risk optimization (EDM03) - Manage risk (APO12)
Phase 5	Review & revision	Monitoring & Review	- Ensure risk optimization (EDM03) - Manage risk (APO12)

- COBIT 5 (Version 2013): Two perspectives of risks are defined by COBIT 5 (Figure 3). The Risk Management Perspective is more accurate to use because it describes how to use COBIT 5 enablers to mitigate information technology risks, and henceforth we selected it [22].
Thus, the risk management perspective uses the two core risk processes of COBIT 5: The first process ensures the optimisation of risks (EDM03) and the second process manages risks (APO12) like presented in Figure 4 [20, 22, 26]. These 2 processes "support the enterprise in obtaining stakeholder value and enterprise objectives while optimising resources and risk" [22].

Five phases compose the methodological approach we propose to follow (Figure 5). As previously stated, this approach takes into consideration the 2 core risk processes defined by COBIT 5 and guidelines of ISO 31000 and COSO ERM. Actually, to define the five phases of the proposed approach, we used the risk management process of ISO 31000 (Figure 4) with minor changes. We chose to use the process of ISO 31000 because it is an end-to-end ERM process and easy to implement [25]. Then the content of each phase is described using the guidelines related to that phase of each framework (Table 2). Below are the details of the development of each phase of the proposed approach:

- The first phase is project scoping: the aim of this phase is to frame and organize the project in terms of defining the stakeholders, the scope, the targets, the schedule, the methodological tool, etc. This phase is created following the (Scope, Context & Criteria) phase of ISO 31000. The content is developed on the basis of the COSO ERM component (Strategy & Objective-setting) and the ISO 31000 phase (Scope, Context & Criteria).
- The second phase is data collection and analysis: the aim of this phase is to collect risk data and structure it by risk category for use in the next phase. Given the importance of IT risk data collection for the whole of the ITRM process, we decided to create a separate phase for data collection,

unlike the ISO 31000 process, which integrates it into the (Scope, Context & Criteria) phase. The content is developed on the basis of three standards: COBIT 5 (APO12 Manage risk), ISO 31000 (Scope, Context & Criteria) and COSO ERM (Strategy & Objective-setting).

- The third phase is the development of the IT risk management framework: the aim of this phase is to map the IT risks associated with the organization. To create this phase, we opted to consolidate the two ISO 31000 phases (Risk Assessment, Risk Treatment) into a single phase, to obtain the IT risk mapping. The content of this phase is based on three standards: COBIT 5 (APO12 Manage risk), ISO 31000 (Risk Assessment, Risk Treatment) and COSO ERM (Performance).
- The fourth phase is change management and communication: the aim of this phase is to disseminate the risk culture within the organization, and to communicate on IT risks in order to better manage them. To create this phase, we merged the two ISO 31000 phases (Recording and Reporting, Communication & Consultation), as the two phases run in parallel. The content of this phase is based on three standards: COBIT 5 (EDM03 Ensure risk optimization, APO12 Manage risk), ISO 31000 (Recording and Reporting, Communication & Consultation) and COSO ERM (Governance & Culture, Information Communication & Reporting).
- The fifth phase is Monitoring & Surveillance: the aim of this phase is to monitor and review IT risks in order to respond in a timely manner with effective measures to limit the extent of losses arising from IT-related events. This phase is based on the Monitoring & Review phase of ISO 31000. The content of this phase is based on three standards: COBIT 5 (EDM03 Ensure risk optimization, APO12 Manage risk), ISO 31000 (Monitoring & Review) and COSO ERM (Review & revision).

4. RESULTS AND DISCUSSION

4.1 Proposition of a roadmap to implement ITRM

Each phase is comprised of several steps, and each step will be described by detailed sub-steps and outputs:

4.1.1 Phase 1: Project scoping

Step 1.1: General directions and shared expectations. This step aims to understand the context, the scope and objectives. The sub-steps to follow are:

- Understand the strategic orientations and the level of maturity of IT risk management
- Conduct interviews with top management in order to: clarify mutual objectives and expectations, exchange on strategic orientations and identify major risks

Step 1.2: Project organization. This step aims to organize the project of development of IT risk management framework. The sub-steps to follow are:

- Define and compose the project team
- Identify the key players and stakeholders
- Draw up the overall project schedule

Output: Scoping document containing: strategic orientations, major risks, objectives and expectations, project team and stakeholders and planning.

Step 1.3: Methodological framework for ITRM. This step aims to identify the methodological framework that will be used to map IT risks. The sub-steps to follow are:

- Definition of the assessment scales for the likelihood, impact, control system and risks criticality
- Definition of the risk matrix and criticality levels

Output: Methodological framework containing: likelihood assessment scale, impact assessment scale, control effectiveness assessment scale and risk matrix and criticality levels.

4.1.2 Phase 2: Data collection and analysis

Step 2.1: Collect and analyse information technology risks' data. This step aims to collect, analyse and synthesize the necessary data related to IT risks allowing the effective identification, analysis and communication of IT risks. The sub-steps to follow are:

- Identify a method for collecting, classifying and analysing IT risk data.
- Analyse the internal and external environment of the company that may have impact on IT risk management.
- Specify IT risks and their mitigation plans related to the industry peers.
- Record data on IT incidents and their impact on the organization.
- Summarize the data collected and highlight IT risk events

Output: Summary document about potential IT risks.

4.1.3 Phase 3: Development of ITRM framework

Step 3.1: Analyse and map IT risks. This step aims to identify known risks and risk attributes (probability of occurrence, impact and response plan) and current control activities. The sub-steps to follow are:

- Identify potential IT risks (the generic scenarios defined by COBIT 5 for risk can be used).
- Identify for each risk macro process, process and category.
- Define risk indicators that allow the monitoring of risks.
- Define specific control activities for each risk.
- Estimate probability of occurrence and impact of risk.
- Assess existing controls, and estimate residual risk.
- Compare residual risk to acceptable risk tolerance and identify risks that may need a response.
- Analyse costs and benefits of potential risk response options.
- Propose the optimal risk response.
- Identify requirements for the implementation of the risk mitigation response.
- Consolidate all identified risks in an overall risk profile.
- Validate the results of risk analysis.

Output: Global risk profile - Risk mapping

Step 3.2: Complete the risk profile. This step aims to identify known risks and risk attributes (probability of occurrence, impact and response plan) and current control activities. The sub-steps to follow are:

- Do the inventory of business processes and identify dependencies on IT applications, services and infrastructures.
- Identify the correspondence between business processes and information technology applications
- Identify the correspondence between business processes and information technology services
- Identify the correspondence between business processes and information technology infrastructures

- Identify critical business processes
- Document IT incidents that have occurred

Output: Correspondence between business processes and information technology applications, information technology processes, information technology infrastructures, critical business processes identified, information technology incident database.

4.1.4 Phase 4: Change management & communication

Step 4.1: Ensure risk culture awareness. This step aims to provide awareness about IT risk management practices and to ensure that they are appropriate and within risk appetite. The sub-steps to follow are:

- Promote a culture of IT risk awareness and empower the organization to proactively identify IT risks, opportunities and potential business impacts.
- Provide and deploy a risk communication plan (covering all levels of the business) in order to promote a culture of IT risk awareness.
- Ensure the integration of ITRM strategy and operations with the ERM system
- Implement an appropriate procedure that explains how to respond quickly to changing risks and report to the appropriate levels of management.
- According to the risk mapping, identify the risk indicators to be monitored and determine the procedures for obtaining and reporting measures.

Output: Plan to communicate about IT risks, API for interfacing between the ITRM system and the ERM system, reporting procedure about IT risks, IT Key Risk Indicator dashboard.

Step 4.2: Communicate and provide risk information. This step aims to provide information on the current status of IT risk exposures periodically and to all relevant stakeholders in order to decide the appropriate action plan. The sub-steps to follow are:

- Prepare and adapt supports to communicate the results of the risk analysis to corresponding stakeholders in order to support business decisions.
- Communicate the current risk profile to corresponding stakeholders, including the effectiveness of incident management, corrective actions and their impact on the risk profile.
- Analyse the results of impartial third-party assessments, internal audits, and quality assurance controls and reflect the impact on the risk profile.

Output: IT Risk analysis report, actualisation of IT risk mapping.

4.1.5 Phase 5: Monitoring and surveillance

Step 5.1: Respond to incidents. This step aims to manage incidents by preparing plans to ensure business continuity and by analysing incidents when occurring. The sub-steps to follow are:

- Prepare, maintain and test Business Continuity Plans (BCP) that specify the steps to be taken when a risk happens that may cause an interruption of business based on the ISO 22301 [32].
- Apply the appropriate response plan to minimize the impact when the risk occurs and update the action plan and its status in the IT incident database
- Rank incidents and compare current exposures with risk tolerance levels. Analyse incidents by specifying root causes, business impacts, additional risk mitigation plan… Communicate the incident analysis to the appropriate stakeholders and update risk profile and IT incident database.

Output: BCP, actualisation of IT incident database and IT risk mapping, IT incident analysis report.

Step 5.2: Monitor ITRM. This step aims to monitor IT risks and report about the monitoring results. The sub-steps to follow are:

- Maintain an inventory of control activities in place to manage risk.
- Monitor mitigation risk plans and their status and determine whether each organizational unit monitors risks within tolerance levels.
- Monitor key risk indicators vs. targets, analyse the gaps and take corrective action to address the underlying causes.
- Monitor the company's progress toward identified objectives.
- Report about the monitoring activities and any risk management issues to the appropriate stakeholders.

Output: Risk monitoring report, updated risk mapping, updated KRI dashboard.

In order to facilitate the deployment of the proposed methodological approach, a practical guide is created stating the different steps to follow.

4.2 Design of RITM 23: The system supporting the roadmap

To design the system RITM 23, the information system that that supports the proposed roadmap, we used UML language. For a better understanding of the structure, functionalities and activities of our system, we present in this sub-section, the context diagram, the use case diagram, the class diagram and the activity diagram of the system.

4.2.1 Context diagram

The context diagram, as in Figure 6, describes the primary and secondary actors interacting with the system. Actors within the system is the Chief Risk Officer (CRO), the administrator and the Enterprise Risk Management system of the organization. The CRO interacts outside the system with experts.

4.2.2 Use case diagram

Use Case diagram, as in Figure 7, serves to describe the main functionalities of the system performed by the CRO (Chief Risk Officer):

- The function of framing the project allows defining strategic orientations, organizing the project and defining the methodological framework
- The function of collecting & synthesizing data allows defining internal & external major facts, collecting IT incidents and risks of the organization & their competitors and summarizing IT risks data
- The function of developing IT risk management framework allows mapping information technology risks of the organization and profiling critical business process & corresponding information technology applications, processes & infrastructures
- The function of communicating & raising risk awareness allows preparing and deploying communication plan, defining risk reporting procedure and identifying key risk indicators to monitor

- The function of monitoring & surveillance allows monitoring risks by defining the Business Continuity Plan for critical risks and updating IT risk mapping, IT incident database, IT key risk indicator dashboard and strategic objectives

All the previous use cases allow uploading documents, displaying and exporting documents.

4.2.3 Class diagram

The relationships between system objects are described using a class diagram, as shown in Figure 8.

The class diagram contains 21 classes and defines the relationships between them. Here are some examples of the classes used:

- Organization class: contains data about the organization, such as its name and whether it is an existing or a new organization.
- Project scoping class: contains data required for scoping the project, such as the project team, schedule, strategic orientations, etc.
- Documents class: contains the various documents loaded into the system.

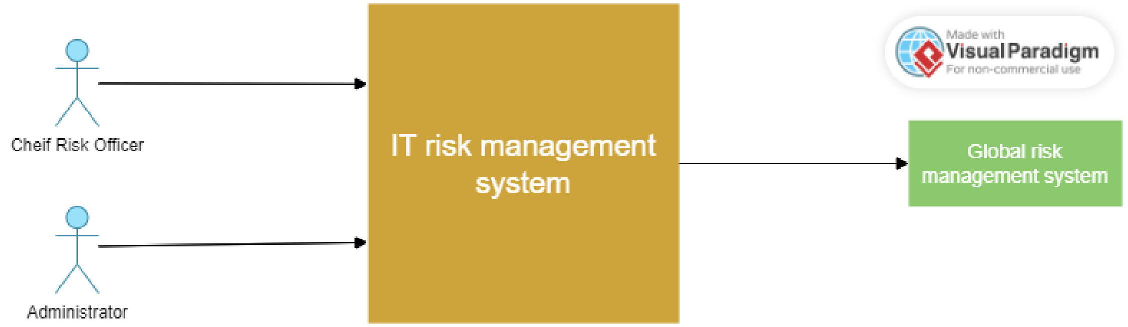

Cheif Risk Officer
Administrator
IT risk management system
Global risk management system
Made with Visual Paradigm For non-commercial use

Figure 6. Context diagram

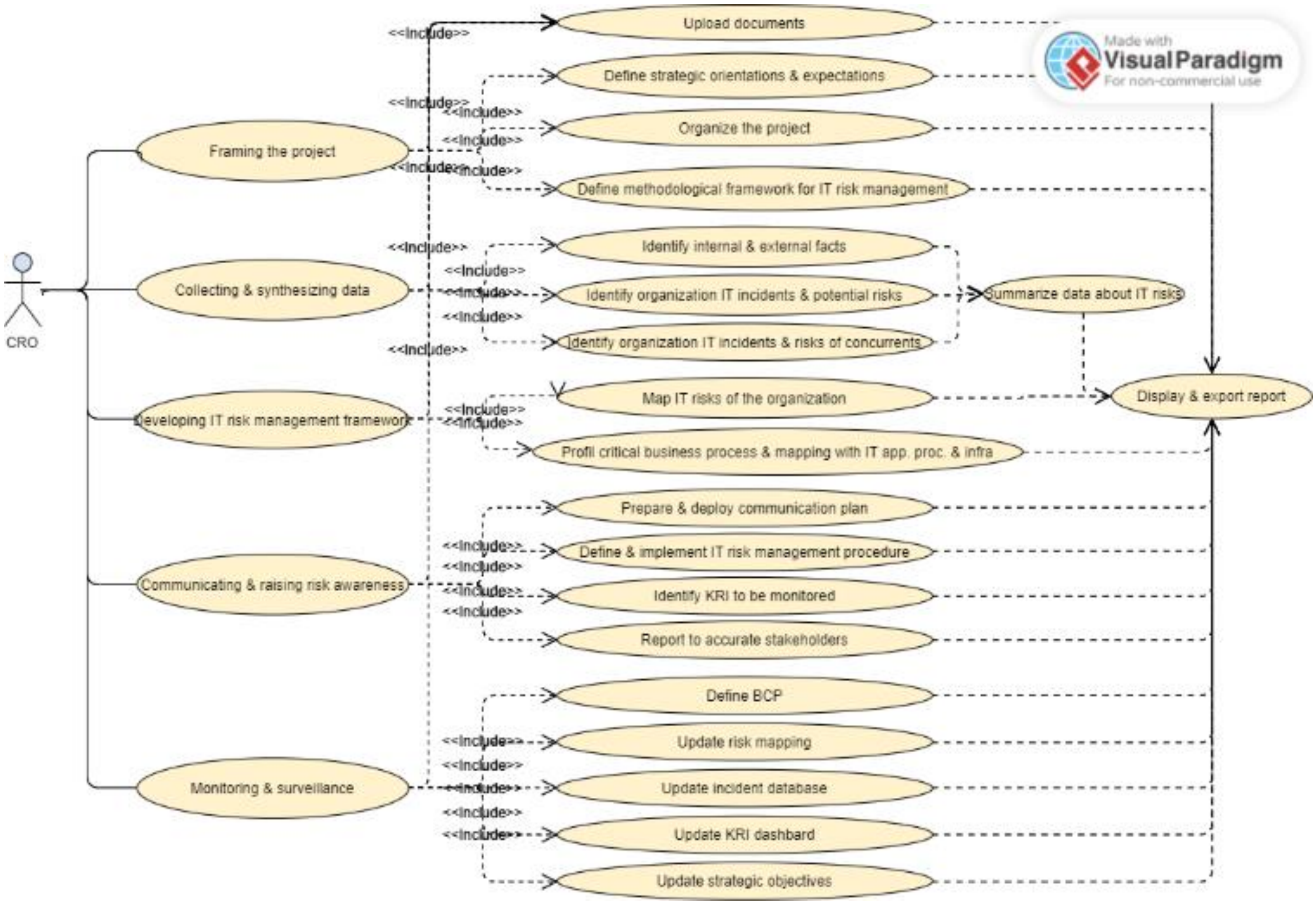

CRO
Framing the project
Collecting & synthesizing data
Developing IT risk management framework
Communicating & raising risk awareness
Monitoring & surveillance
<<Include>>
Upload documents
Define strategic orientations & expectations
Organize the project
Define methodological framework for IT risk management
Identify internal & external facts
Identify organization IT incidents & potential risks
Identify organization IT incidents & risks of concurrents
Summarize data about IT risks
Map IT risks of the organization
Profil critical business process & mapping with IT app, proc. & infra
Display & export report
Prepare & deploy communication plan
Define & implement IT risk management procedure
Identify KRI to be monitored
Report to accurate stakeholders
Define BCP
Update risk mapping
Update incident database
Update KRI dashbard
Update strategic objectives
Made with Visual Paradigm For non-commercial use

Figure 7. Use case diagram

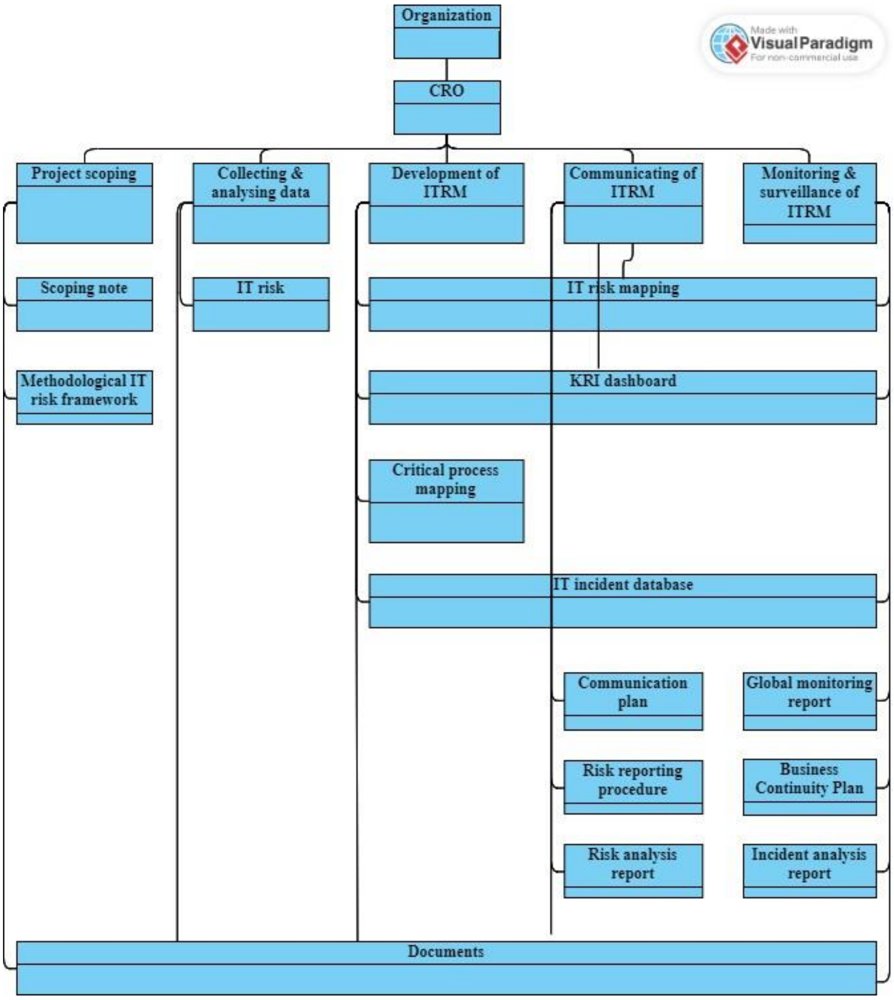


Figure 8. Class diagram

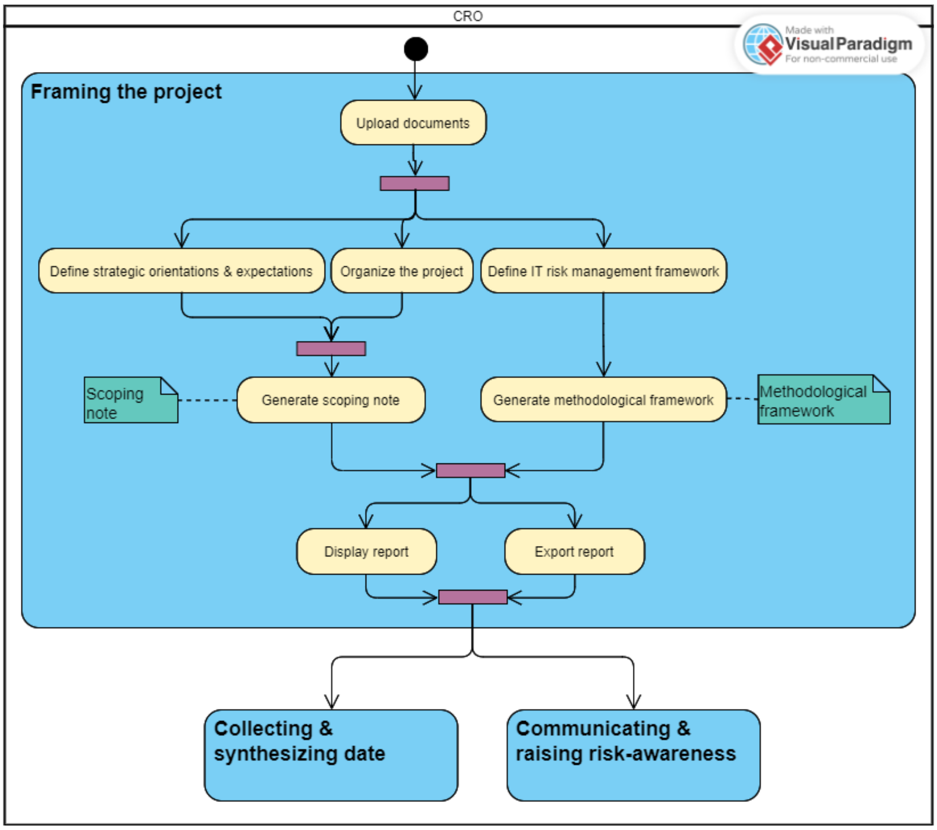

CRO
Framing the project
Upload documents
Define strategic orientations & expectations
Organize the project
Define IT risk management framework
Scoping note
Generate scoping note
Generate methodological framework
Methodological framework
Display report
Export report
Collecting & synthesizing date
Communicating & raising risk-awareness

Figure 9. Activity diagram of phase 1

4.2.4 Activity diagram

The Activity Diagram defines the activities to follow in order to implement Information Technology Risk Management.

In the first phase, as in Figure 9, CRO deploys the different steps needed to define the context of the project and comes up with the generation of report containing the scoping document and the methodological framework. Then the CRO proceeds to the deployment of the activities of phase 2, phase 3, phase 4 and phase 5.

4.3 Development of RITM 23: The system supporting the roadmap

In this section, we'll describe the J2EE system supporting the roadmap. We will present some screenshots while deploying the different steps. As an example, we will integrate screenshots of the home page, phase 2, phase 3 and phase 5.

4.3.1 Home page

In Figure 10, the user is invited to select between a new organization or existing organization which has already deployed the proposed roadmap.

By choosing new organization, the user is invited to precise the name of the organization as in Figure 11, which will be saved in the database.

Once finished, the user clicks on next. In Figure 12, we show the roadmap proposed to implement Information Technology Risk Management in the concerned organization.

4.3.2 Phase 2: Data collection and analysis screens

The first layout of this phase invites the user to upload the documents. These documents will be used while deploying the roadmap, as in Figure 13. The layout of uploading documents is integrated in every phase in order to upload each time the needed documents to analyse and synthesize. Uploaded documents could be visualized, downloaded or deleted.

Next, the user is invited to insert internal facts, external facts, risks of the competitors and internal incidents or potential risks. All the data can be synthesized in the form presented in Figure 14.

4.3.3 Phase 3: Development of IT risk management framework screens

Risk mapping includes all identified risks by specifying the various attributes of the risk (extract of risk mapping in Figure 15), in particular, risk factors, consequences, control activities, macro process, the process, risk category, key risk indicators, control effectiveness, probability of occurrence, impact, risk response options. Noting that the button "Add COBIT 5 generic scenarios" can be used to integrate the IT risk scenarios defined by COBIT 5.

The IT incident database, as shown in Figure 16, lists the various IT incidents that have occurred in the past, with a description of the characteristics of each incident. For example, causes, impact, action plan...

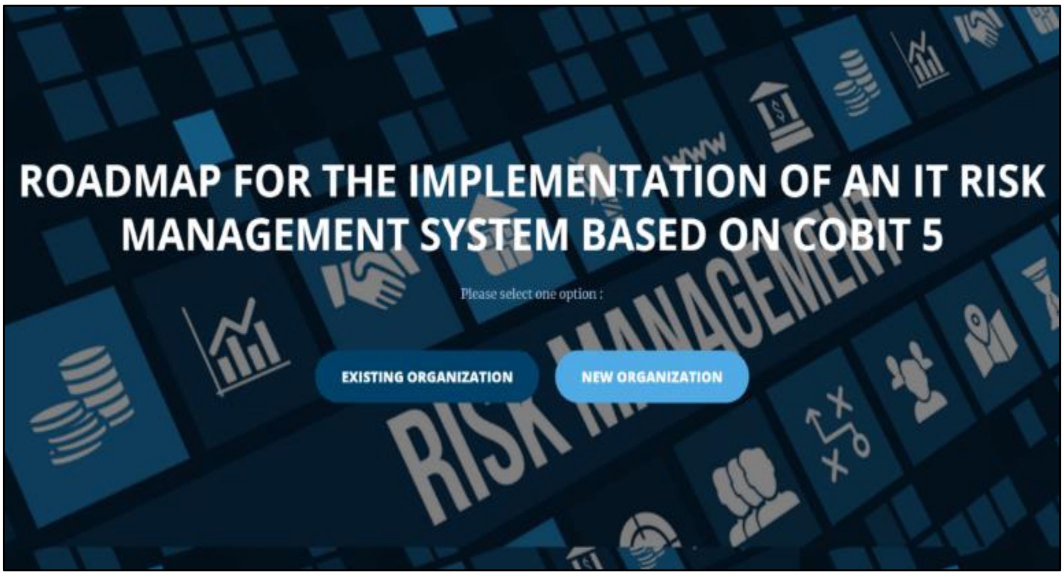
4.3.4 Phase 5: Monitoring and surveillance screens

This phase is dedicated to updating the information entered in the previous phases and producing summary reports as part of risk monitoring and surveillance, in particular:

- Business continuity plan as in Figure 17
- IT incident analysis report as in Figure 18
- Risk monitoring report as in Figure 19

The proposed roadmap and the corresponding system cover the entire process needed for the implementation of IT risk management within organizations. RITM 23 can be deployed in any organization and presents the following advantages:

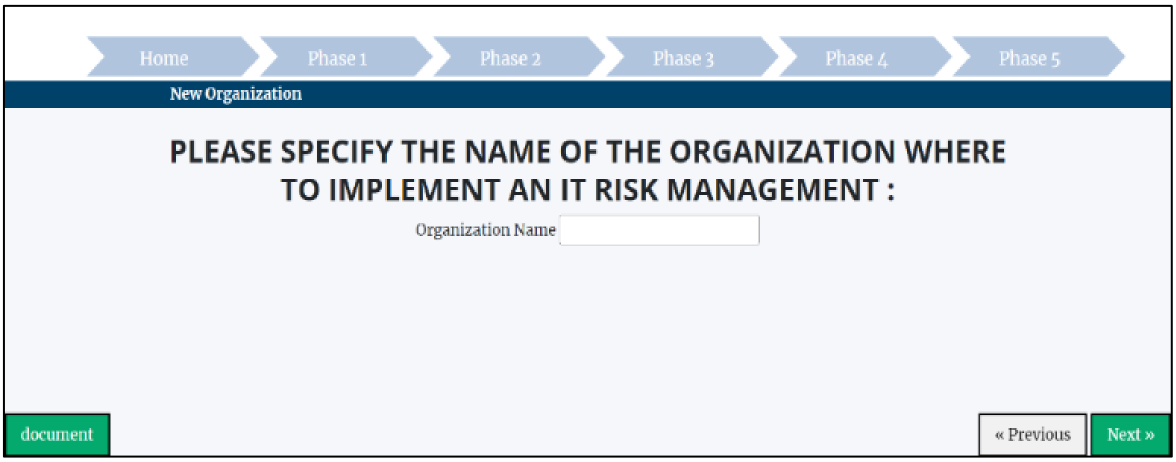
- Structure the 2 core IT risk processes of COBIT 5 into an integrated and structured approach
- Complete the approach with the phase of scoping the project which is missing in COBIT 5 but borrowed from COSO ERM and ISO 31000
- Simplify and sort sequentially steps to follow to Information Technology Risk Management implementation
- Clarify the outputs expected for each step
- Integrate generic IT risk scenarios proposed by COBIT 5 to facilitate the identification of IT risks



ROADMAP FOR THE IMPLEMENTATION OF AN IT RISK MANAGEMENT SYSTEM BASED ON COBIT 5

Please select one option :

Figure 10. Start page

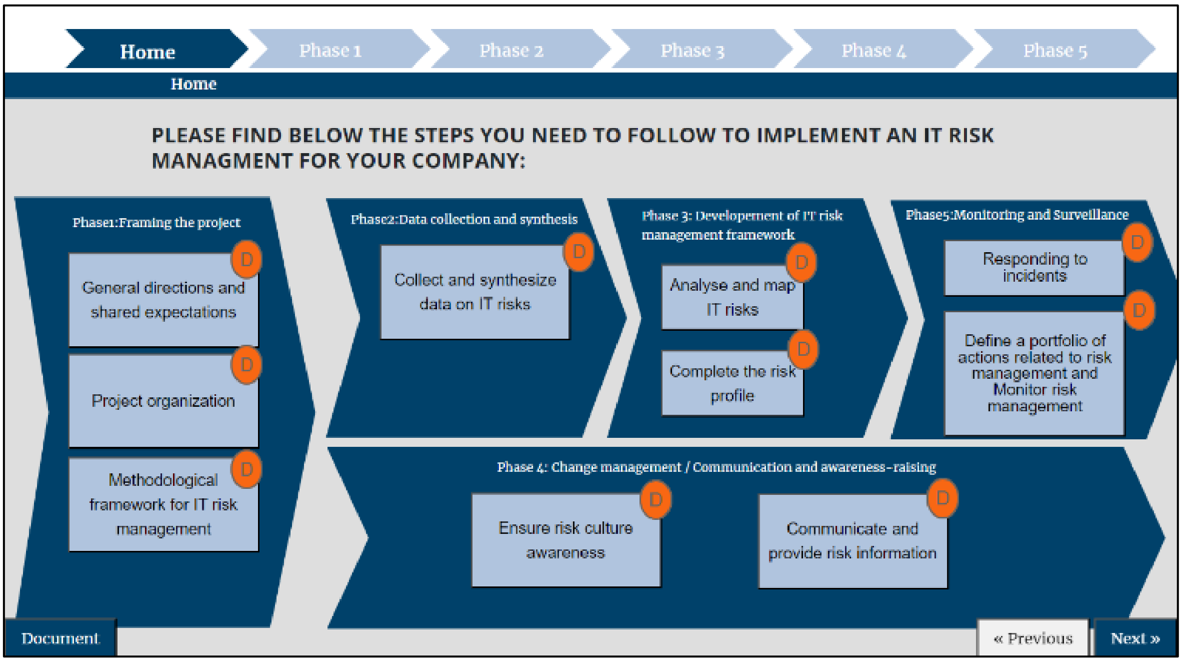


New Organization

PLEASE SPECIFY THE NAME OF THE ORGANIZATION WHERE TO IMPLEMENT AN IT RISK MANAGEMENT :

Organization Name

Figure 11. Screen for specifying the name of the organization



Home

PLEASE FIND BELOW THE STEPS YOU NEED TO FOLLOW TO IMPLEMENT AN IT RISK MANAGMENT FOR YOUR COMPANY:

Phase1:Framing the project

General directions and shared expectations

Project organization

Methodological framework for IT risk management

Phase2:Data collection and synthesis

Collect and synthesize data on IT risks

Phase 3: Development of IT risk management framework

Analyse and map IT risks

Complete the risk profile

Phase5:Monitoring and Surveillance

Responding to incidents

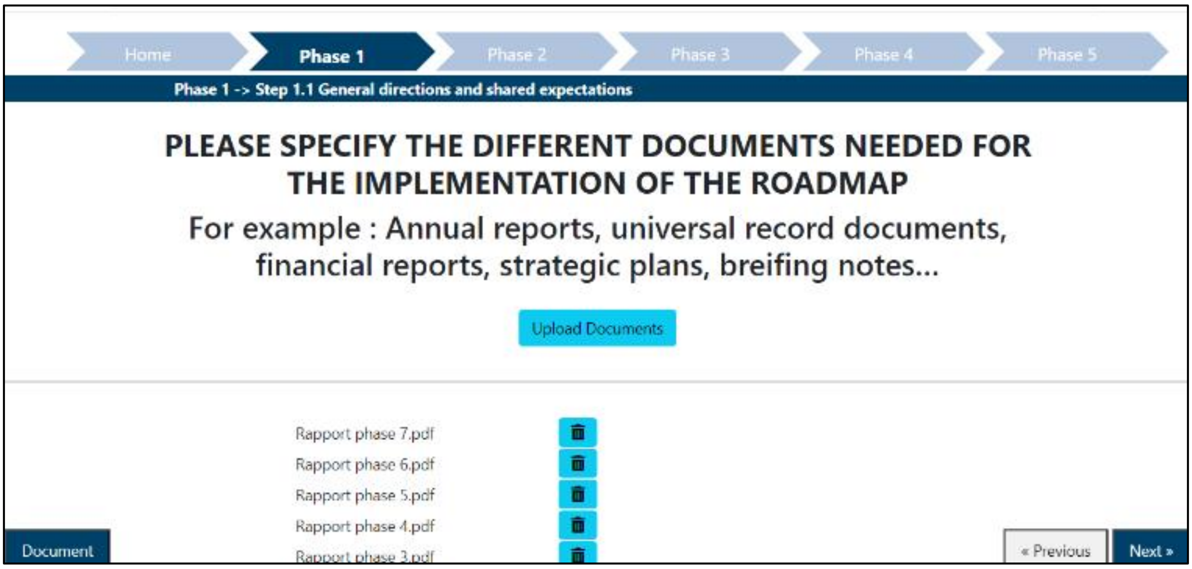
Define a portfolio of actions related to risk management and Monitor risk management

Phase 4: Change management / Communication and awareness-raising

Ensure risk culture awareness

Communicate and provide risk information

Figure 12. Global methodological approach for IT risk management implementation



Phase 1 -> Step 1.1 General directions and shared expectations

PLEASE SPECIFY THE DIFFERENT DOCUMENTS NEEDED FOR THE IMPLEMENTATION OF THE ROADMAP

For example : Annual reports, universal record documents, financial reports, strategic plans, breifing notes...

Rapport phase 7.pdf

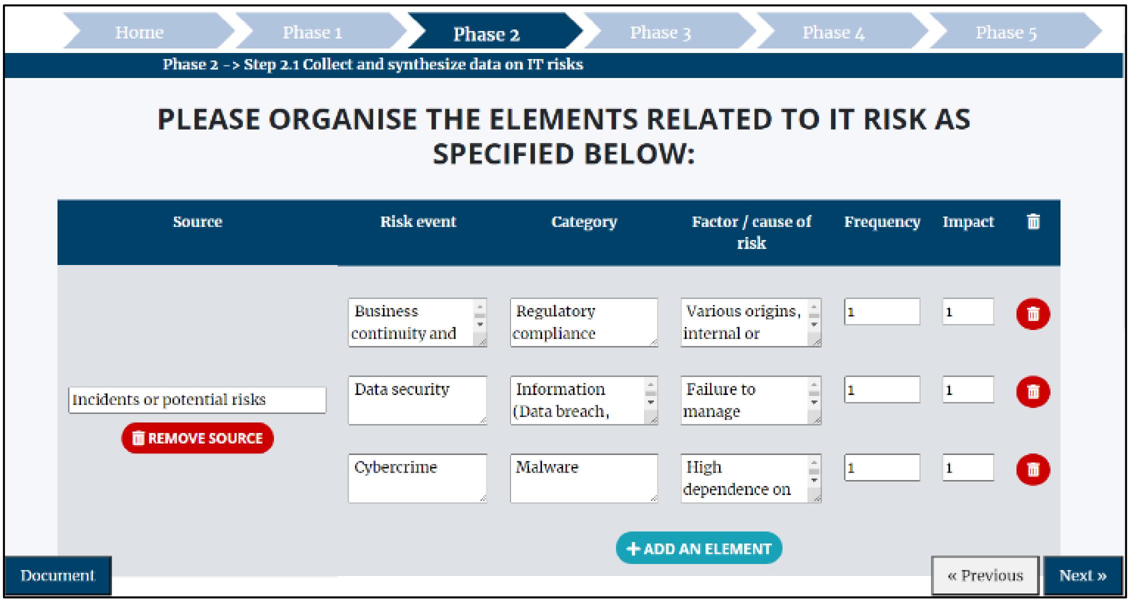
Rapport phase 6.pdf

Rapport phase 5.pdf

Rapport phase 4.pdf

Rapport phase 3.pdf

Figure 13. Upload documents screen

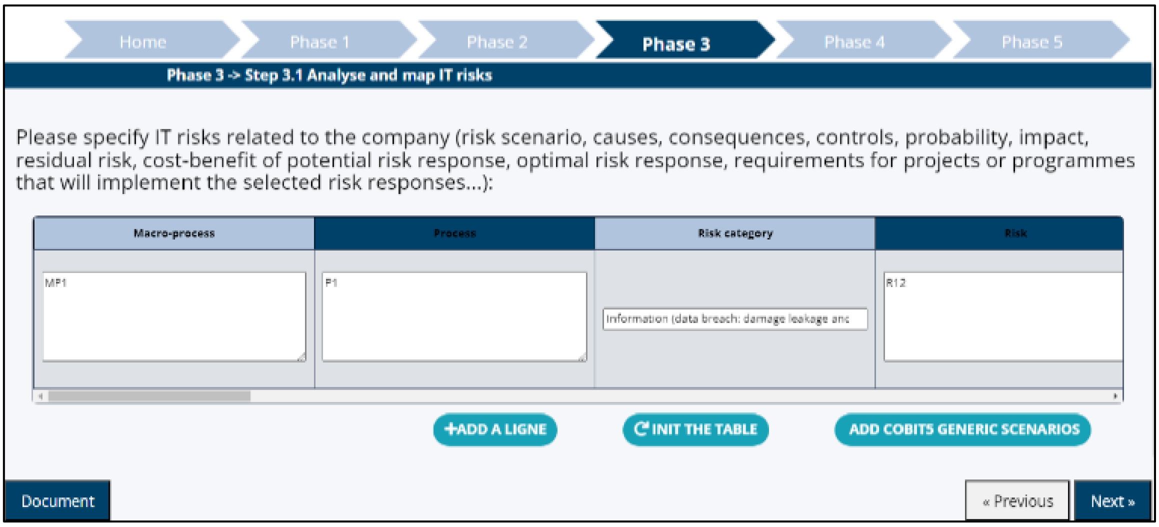


Phase 2 -> Step 2.1 Collect and synthesize data on IT risks

PLEASE ORGANISE THE ELEMENTS RELATED TO IT RISK AS SPECIFIED BELOW:

Source	Risk event	Category	Factor / cause of risk	Frequency	Impact
Incidents or potential risks	Business continuity and	Regulatory compliance	Various origins, internal or	1	1
	Data security	Information (Data breach,	Failure to manage	1	1
	Cybercrime	Malware	High dependence on	1	1

Figure 14. Screen synthesizing data collected about IT risks

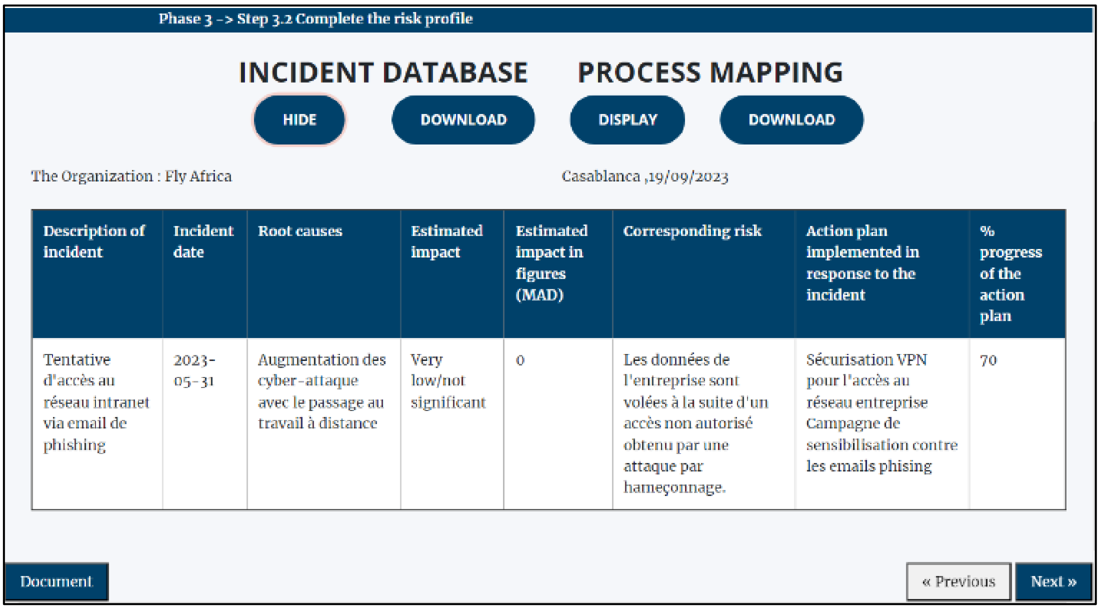


Phase 3 -> Step 3.1 Analyse and map IT risks

Please specify IT risks related to the company (risk scenario, causes, consequences, controls, probability, impact, residual risk, cost-benefit of potential risk response, optimal risk response, requirements for projects or programmes that will implement the selected risk responses...):

Macro-process	Process	Risk category	Risk
MP1	P1	Information (data breach: damage leakage anc	R12

Figure 15. Extract of risk mapping


Phase 3 -> Step 3.2 Complete the risk profile

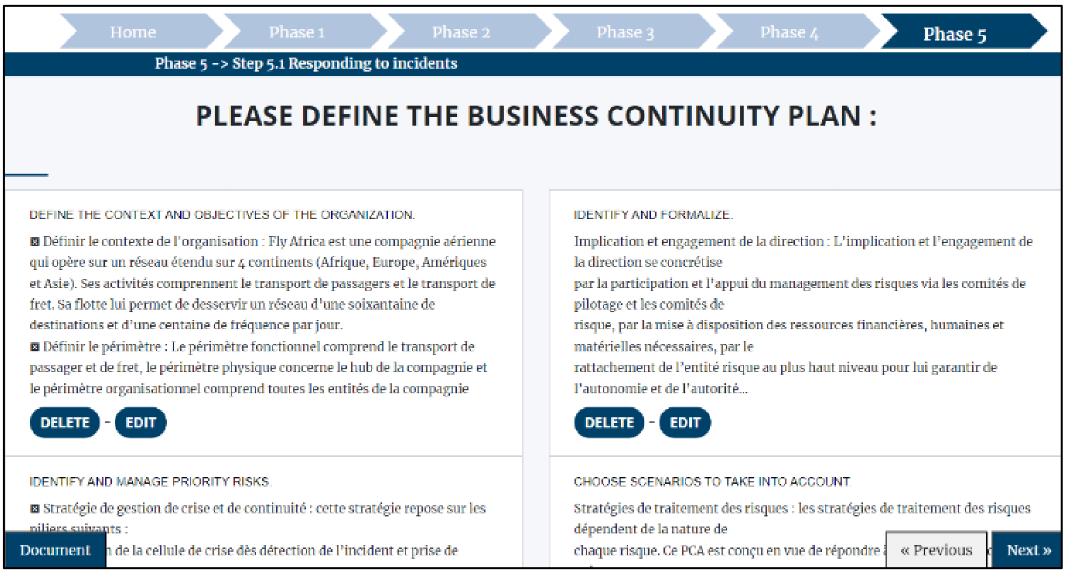
INCIDENT DATABASE   PROCESS MAPPING

The Organization : Fly Africa

Casablanca ,19/09/2023

Description of incident	Incident date	Root causes	Estimated impact	Estimated impact in figures (MAD)	Corresponding risk	Action plan implemented in response to the incident	% progress of the action plan
Tentative d'accès au réseau intranet via email de phishing	2023-05-31	Augmentation des cyber-attaque avec le passage au travail à distance	Very low/not significant	0	Les données de l'entreprise sont volées à la suite d'un accès non autorisé obtenu par une attaque par hameçonnage.	Sécurisation VPN pour l'accès au réseau entreprise Campagne de sensibilisation contre les emails phising	70

Figure 16. IT incident database



Phase 5 -> Step 5.1 Responding to incidents

PLEASE DEFINE THE BUSINESS CONTINUITY PLAN :

DEFINE THE CONTEXT AND OBJECTIVES OF THE ORGANIZATION.

☒ Définir le contexte de l'organisation : Fly Africa est une compagnie aérienne qui opère sur un réseau étendu sur 4 continents (Afrique, Europe, Amériques et Asie). Ses activités comprennent le transport de passagers et le transport de fret. Sa flotte lui permet de desservir un réseau d'une soixantaine de destinations et d'une centaine de fréquence par jour.

☒ Définir le périmètre : Le périmètre fonctionnel comprend le transport de passager et de fret, le périmètre physique concerne le hub de la compagnie et le périmètre organisationnel comprend toutes les entités de la compagnie

IDENTIFY AND FORMALIZE.

Implication et engagement de la direction : L'implication et l'engagement de la direction se concrétise
par la participation et l'appui du management des risques via les comités de pilotage et les comités de
risque, par la mise à disposition des ressources financières, humaines et matérielles nécessaires, par le
rattachement de l'entité risque au plus haut niveau pour lui garantir de l'autonomie et de l'autorité...

IDENTIFY AND MANAGE PRIORITY RISKS.

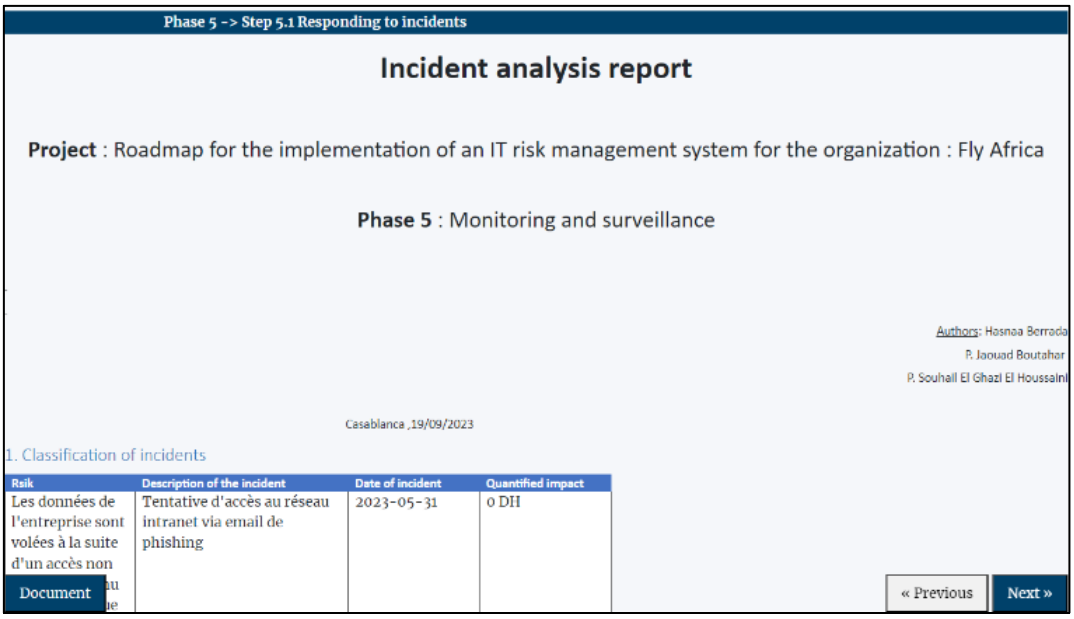
☒ Stratégie de gestion de crise et de continuité : cette stratégie repose sur les piliers suivants :

n de la cellule de crise dès détection de l'incident et prise de

CHOOSE SCENARIOS TO TAKE INTO ACCOUNT.

Stratégies de traitement des risques : les stratégies de traitement des risques dépendent de la nature de
chaque risque. Ce PCA est conçu en vue de répondre à

Figure 17. Business continuity plan



Phase 5 -> Step 5.1 Responding to incidents

Incident analysis report

Project : Roadmap for the implementation of an IT risk management system for the organization : Fly Africa

Phase 5 : Monitoring and surveillance

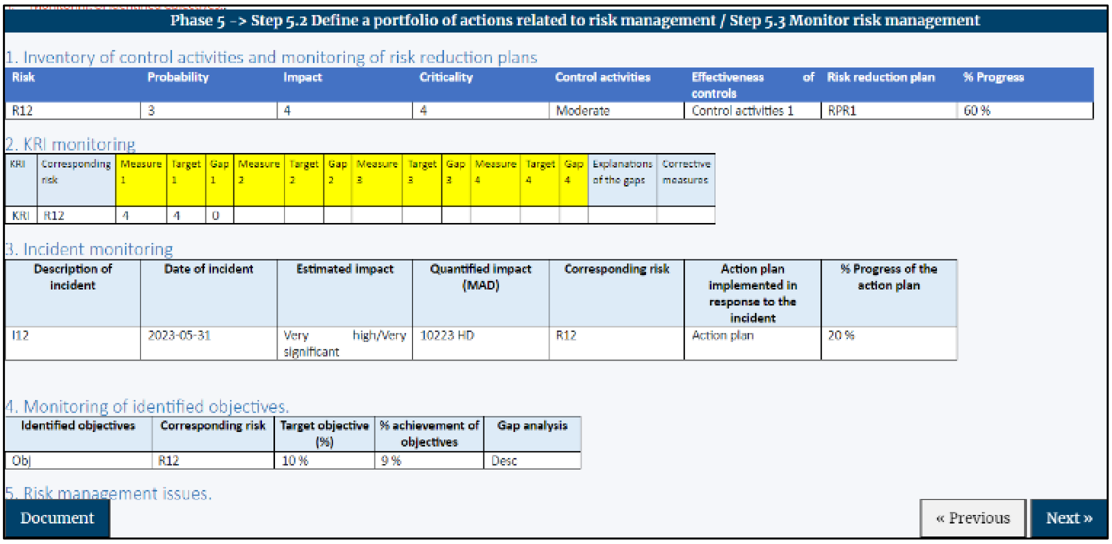
Authors: Hasnaa Berrada
P. Jaouad Boutahar
P. Souhail El Ghazi El Houssaini

Casablanca ,19/09/2023

1. Classification of incidents

Rsik	Description of the incident	Date of incident	Quantified impact
Les données de l'entreprise sont volées à la suite d'un accès non	Tentative d'accès au réseau intranet via email de phishing	2023-05-31	0 DH

Figure 18. Incident analysis report



Phase 5 -> Step 5.2 Define a portfolio of actions related to risk management / Step 5.3 Monitor risk management

1. Inventory of control activities and monitoring of risk reduction plans

Risk	Probability	Impact	Criticality	Control activities	Effectiveness of controls	Risk reduction plan	% Progress
R12	3	4	4	Moderate	Control activities 1	RPR1	60 %

2. KRI monitoring

KRI	Corresponding risk	Measure 1	Target 1	Gap 1	Measure 2	Target 2	Gap 2	Measure 3	Target 3	Gap 3	Measure 4	Target 4	Gap 4	Explanations of the gaps	Corrective measures
KRI	R12	4	4	0											

3. Incident monitoring

Description of incident	Date of incident	Estimated impact	Quantified impact (MAD)	Corresponding risk	Action plan implemented in response to the incident	% Progress of the action plan
I12	2023-05-31	Very high/Very significant	10223 HD	R12	Action plan	20 %

4. Monitoring of identified objectives.

Identified objectives	Corresponding risk	Target objective (%)	% achievement of objectives	Gap analysis
Obj	R12	10 %	9 %	Desc

5. Risk management issues.

Figure 19. Risk monitoring report

5. CONCLUSIONS

In this article, we have proposed an integrated, simplified and holistic roadmap to an ITRM implementation as well as the system RITM 23 supporting this roadmap. By combining different standards (ISO 31000, COSO ERM and COBIT 5), we have designed a whole framework that involves Information Technology Risk Management processes and information technology governance processes. The proposed roadmap comprises five phases: The first phase starts with scoping the project, then collecting and analysing data related to IT risks. The next phase is used to develop ITRM framework. The last phase serves to monitor IT risks. Given the importance of communication and change management, these are deployed throughout the project. By following this roadmap, each organization will be able to put in place the process of ITRM and generate the necessary outputs like IT risk mapping, IT risk analysis report, IT incident analysis report, Business Continuity Plan and others. The system supporting the roadmap simplifies further the deployment of IT risk management. It was designed by UML language through creating the context diagram, the use case diagram, the class diagram and the activity diagram. The development of the system was supported by J2EE and some screenshots were presented.

The proposed roadmap and the corresponding system cover the entire process needed for the implementation of ITRM within organizations. Thus, RITM 23 can be deployed in any organization. However, it is necessary to note that the deployment of the roadmap needs the contribution of business experts. Perhaps, the introduction of artificial intelligence could further automate the process of implementation of IT risk management within organizations.

REFERENCES

[1] Poupart-Lafarge, O. (2010). Cadre de référence sur les dispositifs de gestion des risques et de contrôle interne, France: AMF Publication.

[2] Ferris, S.P., Javakhadze, D., Rajkovic, T. (2017). CEO social capital, risk-taking and corporate policies. Journal of Corporate Finance, 47: 46-71. https://doi.org/10.1016/j.jcorpfin.2017.09.003

[3] IRM. (2022). Professional standards in Risk Management. London: IRM (Institute of Risk Management).

[4] O'Brien, J.A. (1996). Management Information Systems: Managing Information Technology in the Networked Enterprise. McGraw-Hill.

[5] Saeidi, P., Saeidi, S.P., Sofian, S., Saeidi, S.P., Nilashi, M., Mardani, A. (2019). The impact of Enterprise Risk Management on competitive advantage by moderating role of information technology. Computer Standards & Interfaces, 63: 67-82. https://doi.org/10.1016/j.csi.2018.11.009

[6] Wijanarka, H. (2014). IT risk management to support the realization of IT value in public organizations. In 2014 International Conference on ICT For Smart Society (ICISS), Bandung, Indonesia, pp. 113-117. https://doi.org/10.1109/ICTSS.2014.7013160

[7] ProcessUnity. (2022). Aligning internal cybersecurity practices with external third-party risk management. ProcessUnity, United States.

[8] HOF, R. (2017). Nearly 5-hour Amazon Web Services outage highlights dependence on one cloud giant. SiliconANGLE.

[9] Langewiesche, W. (2019). What really brought down the Boeing 737 Max. The New York Times Magazine, 18: 1-26.

[10] Hamblen, M. (2020). Killer software: 4 lessons from the deadly 737 MAX crashes. FIERCE Electronics.

[11] Isidore, C. (2022). A 737 crashed in China. What we know about the plane. CNN Business.

[12] Dolfing, H. (2019). Case Study 4: The $440 Million Software Error at Knight Capital. https://www.henricodolfing.com/2019/06/project-failure-case-study-knight-capital.html.

[13] Suroso, J.S., Rahadi, B. (2017). Development of IT risk management framework using COBIT 4.1, implementation in IT governance for support business strategy. In Proceedings of the 1st International Conference on Education and Multimedia Technology, pp. 92-96. https://doi.org/10.1145/3124116.3124134

[14] ISO. (2018). ISO 31000 - Management du risqué. ISO Publication.

[15] ISO. (2009). ISO Guide 73: Risk management - Vocabulary. ISO Publication.

[16] COSO. (2013). Internal Control - Integrated Framework. COSO Publication.

[17] Renard, J. (2012). Comprendre et Mettre en Oeuvre le Contrôle Interne. Paris: Eyrolles.

[18] ISO. (2018). ISO/IEC 27005: 2018 Information technology - Security techniques - Information security risk management. ISO Publication.

[19] ISO. (2018). ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO Publication.

[20] ISACA. (2012). COBIT 5: A business framework for Governance and Management of enterprise IT. USA: ISACA Publication.

[21] ISACA. (2014). Relating the Coso Internal Control - Integrated Framework and Cobit. ISACA Publication, USA.

[22] ISACA. (2013). COBIT 5 for Risk. USA: ISACA Publication.

[23] Al-Ahmad, W., Mohammed, B. (2015). A code of practice for effective information security risk management using COBIT 5. In 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa, pp. 145-151. https://doi.org/10.1109/InfoSec.2015.7435520

[24] Berrada, H., Boutahar, J., El Houssaïni, S.E.G. (2021). Simplified IT risk management maturity audit system based on "COBIT 5 for Risk". International Journal of Advanced Computer Science and Applications, 12(8): 641-652. https://doi.org/10.14569/ijacsa.2021.0120875

[25] Sutra, G. (2018). Management des risques une approche stratégique. Afnor Editions.

[26] ISACA. (2012). COBIT 5: Enabling Processes. USA: ISACA Publication.

[27] Osinovskaya, I., Riska, P., (2015). Management decision-making under risk. Economy and Entrepreneurship, 767-770.

[28] El ghazi El Houssaïni, S., Youssfi, K., Boutahar, J. (2016). CAT5: A tool for measuring the maturity level of information technology governance using COBIT 5 framework. International Journal of Advanced Computer

Science and Applications, 7(2): 385-391.

[29] Astuti, H.M., Muqtadiroh, F.A., Darmaningrat, E.W.T., Putri, C.U. (2017). Risks assessment of information technology processes based on COBIT 5 framework: A case study of ITS service desk. Procedia Computer Science, 124: 569-576. https://doi.org/10.1016/j.procs.2017.12.191

[30] Wulandari, S.A., Dewi, A.P., Pohan, M.R., Sensuse, D.I., Mishbah, M. (2019). Risk assessment and recommendation strategy based on COBIT 5 for risk: Case study SIKN JIKN helpdesk service. Procedia Computer Science, 161: 168-177. https://doi.org/10.1016/j.procs.2019.11.112

[31] COSO. (2017). Enterprise Risk Management - Integrating with Strategy and Performance. COSO.

[32] ISO. (2019). ISO 22301:2019 Sécurité et résilience - Systèmes de management de la continuité d'activité - Exigences. ISO Publication.