International Journal of Safety and Security Engineering
Vol.14, No. 2, April, 2024, pp. 411-419
Journal homepage: http://iieta.org/journals/ijsse

MART 23: A Tool to Audit Information Technology Risk Management Maturity

Hasnaa Berrada*, Jaouad Boutahar, Souhaïl El Ghazi El Houssaïni

Systems Architectures and Networks Team, EHTP - Ecole Hassania des Travaux Publics - Hassania School of Public Works, Casablanca 20230, Morocco

Corresponding Author Email: hasnaa.berrada@gmail.com

https://doi.org/10.18280/ijsse.140209

Received: 31 October 2023
Revised: 9 April 2024
Accepted: 16 April 2024
Available online: 26 April 2024

Keywords:
IT risk management, COBIT 5, maturity audit tool, analysis axes, maturity scale, maturity audit report

ABSTRACT

In recent years and due to different crises (financial crises, epidemic crises, politic crise), organizations have turned their attention to searching best practices in order to better manage inherent risks. Actually, every organization is now obliged to take risks so as to grow and even to survive. Under these conditions, it is vital to correctly manage potential risks to the business, otherwise, if these risks occur, organizations may not be able to reach their objectives. From another side, all businesses rely on information technology so its related risks should be well managed. Consequently, and to audit the maturity of information technology risk management (ITRM), we developed a system named MART 23, built on using best practices of COBIT 5. In fact, COBIT 5 like other standards presents some guidelines for risk management / information technology risk management, but none of them offer an operational approach and tool for auditing, assessing and improving ITRM maturity in organizations. In the following article, the MART 23 system is presented to audit ITRM maturity, through UML design and some layouts.

1. INTRODUCTION

In a dynamic, globalized and constantly changing environment, risk is an integral part of organizational processes and activities [1]. Mergers & acquisitions, partnerships, globalization and ongoing technological developments are all examples of risk-generating factors [1] and challenges facing organizations [2]. In this regard, organizations are giving more and more importance to risk management, which can be human, commercial, economic or political in nature [2].

The use of IT in a company, to adequately reap the benefits it brings, it must be accompanied by effective and efficient management of IT-related risks. Otherwise, it may hinder the attainment of corporate objectives [3]. ITRM should be taken into account in a holistic approach to enterprise risk management, hence a framework for integrating IT risks into ERM is needed [4, 5].

To this end, standards and guidelines have been drawn up for risk management, focusing on ITRM and information security. Noting for example COSO [6, 7], a reference in internal control. In 2017, COSO ERM is a form of COSO dedicated to enterprise risk management (ERM) [8]. There is also, ISO 31000 [9, 10], which is a standard that gets bases and guides for risk management put forward, besides implementation processes at different levels. From the other side, we consider COBIT, a framework in IT management and governance [11, 12]. In its version of COBIT 5, a dedicated publication was published to deal with information technology risk management [13, 14]. However, this publication is considered hard to implement and needs integrated and structured approach to guide organizations that wants to establish ITRM [15-18]. In addition to the difficulty of implementing ITRM using COBIT 5 or other available standards, none of existing standards offer an operational approach and tool for auditing, assessing and improving IT risk management maturity within organizations.

Research works are in progress to contribute in filling this gap and propose a holistic system to ITRM maturity audit. Actually, we have already published an article, cited in the study of Berrada et al. [19], that describes a methodological approach to audit the maturity of ITRM. In the continuity of these research works, we propose, in this article, to present an operational tool to audit the maturity of ITRM. The tool was developed based on an integrated methodological approach to audit the ripeness of ITRM previously detailed in another article [19].

The beginning of this article describes briefly the methodological approach used to audit the maturity of ITRM. Then, the UML design of the system is presented, and some layouts are described. The last section is dedicated for the conclusion and perspectives.

2. METHODOLOGY

In order to implement an ITRM maturity audit system in an institution, it is necessary to audit the overall organization's ITRM environment. To this end, we propose using a way rooted on the COBIT 5 framework [11, 13, 20].

COBIT 5 defines seven enablers (Figure 1) [11, 13] which describe the different pillars of an institution needed for ITRM

and governance.

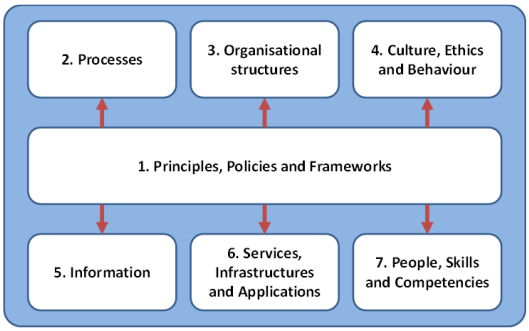


Figure 1. A reminder of the 7 enablers of COBIT 5 [11]

COBIT 5 put forward guidelines and details how each enabler affects the overall governance and management of the risk function. As such, it defines:

- What are the bases, protocols and standards needed to govern and manage risk, for example: the principle of balancing the cost and benefit of IT risk, information security policy.
- What processes are needed to identify and support the risk function, and to govern and manage risk, e.g. APO12 for managing Risk, EDM03 for optimizing Risk.
- What organizational structures are needed to establish an effective risk management and governance, e.g. the corporate risk committee, the risk entity.
- What culture, ethics and behaviours need to be conveyed within the organization in order to better govern and manage risks, e.g.: raising awareness of risk policy, enabling the risk acceptance option for minor risks.
- The information flows necessary for risk management and governance, e.g. communication plan, risk profile…
- What services, infrastructures and applications are needed to govern and manage risks, e.g. crisis management, GRC (Governance, Risk, Compliance) tools.
- What people and skills are needed to set up and manage a risk function effectively, e.g. risk managers, analytical skills…

In line with the 7 enablers defined by COBIT 5, we propose a methodological approach called MART 23, broken down into 7 phases. This methodological approach will enable us to audit the maturity of IT risks within institutions.

The seven phases of the methodological approach to be used for the ITRM maturity audit within an organization are as follows:

2.1 Phase 1 - Auditing the maturity of principles, policies and frameworks in terms of ITRM

This phase, in line with the enabler 1 of COBIT 5 (Principles / bases, policies / protocols and frameworks / standards), aims to audit the maturity of existing bases, protocols and standards within an organisation. For example, in this phase we can assess the maturity of the core IT risk policy according to predefined analysis axes (Existence, Scope, Roles and Responsibilities…) and state the action plan to be set up so to improve the maturity level of the core IT risk policy.

2.2 Phase 2 – Auditing the maturity of ITRM processes

This phase, in line with the enabler 2 of COBIT 5 (Processes), aims to audit the maturity of existing processes within an organisation. For example, in this phase we can evaluate the maturity of the process "Ensure risk optimization" according to predefined rating system (Incomplete process, Process executed, Managed process.) and state the action plan to be set up so that it improves the maturity level of the process "Ensure risk optimization".

2.3 Phase 3 – Auditing the maturity of organizational structures in terms of ITRM

This phase, in line with the enabler 3 of COBIT 5 (Organizational structures), aims to audit the maturity of existing organizational structures within an organisation. For example, in this phase we can assess the maturity of the ERM committee according to predefined analysis axes (Level of importance, Span of control, Risk-based decisions.) and state the action plan to be set up so to improve the maturity level of the ERM committee.

2.4 Phase 4 – Auditing the maturity of culture, ethics and behaviour in terms of IT risk management

This phase, in line with the enabler 4 of COBIT 5 (culture, ethics and behaviour), aims to audit the maturity of existing behaviours within an organisation. For example, in this phase we can evaluate the maturity of recognizing the value of risk, as a behaviour, according to predefined analysis axes (Communication, Awareness, Rules and norms…) and state the action plan to be set up so to improve the maturity level of that behaviour within the institution.

2.5 Phase 5 – Auditing the maturity of information in terms of ITRM

This phase, in line with the enabler 5 of COBIT 5 (Information), aims to audit the maturity of existing types of information within an organisation. For example, in this phase we can weigh the maturity of the risk profile, as an information, according to predefined analysis axes (Existence, Information carrier or media, Information access channel…) and state the action plan to be set up so to enhance the maturity level of the risk profile.

2.6 Phase 6 – Auditing the maturity of services, infrastructures and applications in terms of ITRM

This phase, in line with the enabler 6 of COBIT 5 (Services, Infrastructures and Applications), aims to audit the maturity of existing services, infrastructures and applications within an organisation. For example, in this phase we can evaluate the maturity of the Crisis management services according to predefined analysis axes (Existence, Functional, Architecture principles…) and state the action plan to be set up in order to improve the maturity level of that service.

2.7 Phase 7 – Auditing the maturity of people, skills and competencies in terms of ITRM

This phase, in line with the enabler 7 of COBIT 5 (people, skills and competencies), aims to audit the maturity skills & competences of existing organizational roles within an organisation. For example, in this phase we can evaluate the maturity of the Chief Compliance Officer according to

predefined analysis axes (Leadership skills, Analytical capability, Critical thinking.) and state the action plan to be set up in order to improve the maturity level of skills & competences of that organizational role.

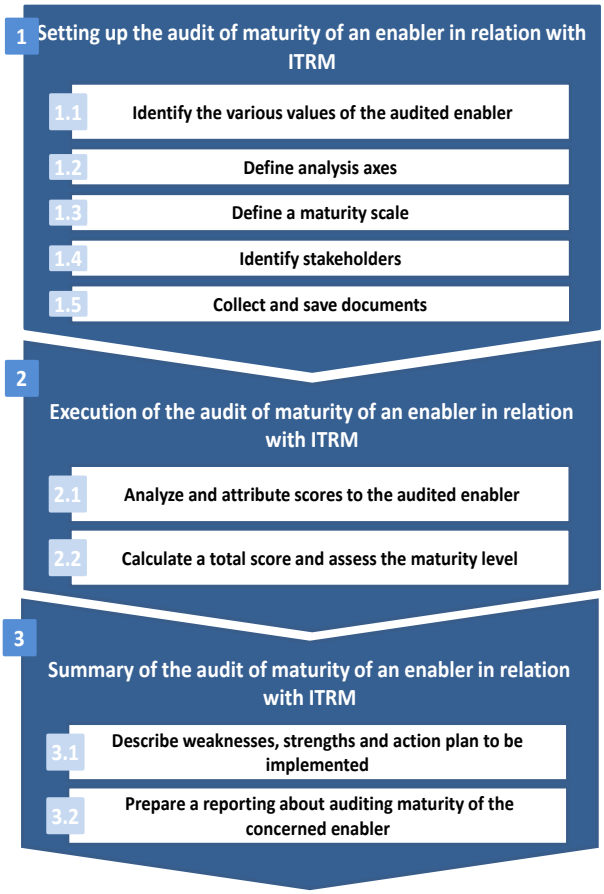


Figure 2. Steps and sub-steps of the methodological approach to assess ITRM maturity, to be adopted for each phase

For each phase, all the steps and sub-steps to be followed to assess the level of maturity of each dimension, in terms of IT risk management, are described in Figure 2.

MART 23, the proposed COBIT 5-based methodological approach to ITRM maturity auditing, can be deployed and adapted to all organizations in different sectors.

For further information about the proposed approach please refer to the article cited in the study of Berrada et al. [19].

3. MART 23: A TOOL TO ITRM MATURITY AUDIT

3.1 Design of MART 23

The approach adopted for the design of the maturity audit system MART 23 consists of a unified development process built around UML (Unified Modeling Language). The latter is the most widely used modeling language for designing object-oriented software.

During the design phase, user requirements and the different stakeholders are identified, interactions of the stakeholders with the system are described, and the different diagrams required to develop the system are drawn up.

3.1.1 Context diagram

The context diagram (Figure 3) describes the main and secondary actors who interact with the system. The actors within the system are the IT auditor and the business manager. The overall ITRM maturity audit system comprises the 7 components to be audited:

- Principles, policies and frameworks
- Processes
- Organizational structures
- Culture, ethics and behaviors
- Information
- Services, infrastructures and applications
- People, skills and competencies

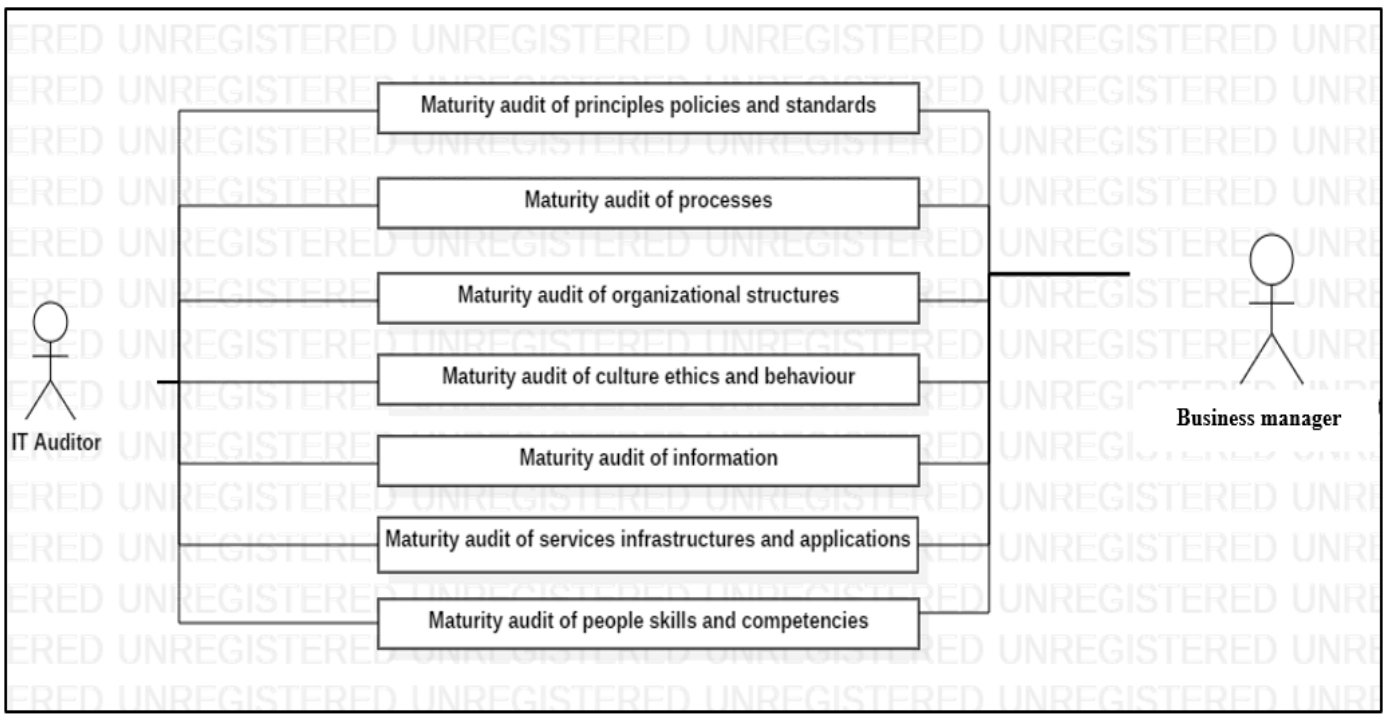


Figure 3. Context diagram detailing actors that interacts with MART 23 (designed with the test version of StarUML software)

3.1.2 Use case diagram

The use case diagram shows the functional relationships between the actors and the system under study. It provides a coherent description of all possible views of the system. The use case diagram shown in this section (Figure 4) summarizes the main functionalities of our information system.

In fact, the IT auditor can unfold 3 use cases:

- Planning the maturity audit: this function includes the sub-functions of facilitator value management, analysis axis management and stakeholder management. These sub-functions give rise to the functionalities of managing the overall maturity level and collecting and saving documents.

- Execution of the maturity audit: this function includes the analysis and scoring sub-function, resulting in the calculation of the total score and evaluation of the maturity level.

- Synthesis of the maturity audit: this function includes the sub-functions of describing strengths and weaknesses, and consolidating the final maturity audit report for the facilitator concerned.

3.1.3 Activity diagram

The activity diagram is a representation close to the flowchart: the description of a use case by an activity diagram corresponds to its algorithmic translation. An activity is the execution of part of a use case. The activity diagram for our system looks like shown in Figure 5.

The IT auditor begins by managing the different values of the enabler to be audited, by adding, modifying and deleting values. Then, the IT auditor can manage the analysis axes (add, modify and delete). Next, the IT auditor manages the stakeholders and the overall maturity scale. After that, the IT auditor collects and saves the documents required for the audit, in collaboration with the business managers concerned. Following these activities, the IT auditor analyses the documents collected and assigns scores to the various values of the enabler concerned, according to the analysis axes selected. The total score is automatically calculated and the maturity level assessed. The IT auditor then describes the strengths, the weaknesses and the related action plan, and generates the reporting of auditing the maturity of the enabler concerned.

3.1.4 Class diagram

The class diagram describes the system in an abstract way, in terms of classes, structure and associations. The class diagram is created using object-relational mapping, or ORM. This method creates a correspondence between the relational database and the language objects, associating each class with a table and each class attribute with a table field.

The class diagram (Figure 6) of our maturity audit system contains 3 packages and 10 classes as follows:

- The first package comprises the classes related to audit planning, namely:
  * Analysis axes
  * Enabler values
  * Stakeholders
  * Global maturity scale
  * Documents
- The second package includes classes related to audit execution, namely:
  * Scores
  * Maturity level
- The third package includes classes related to the audit summary, namely:
  * Strengths, weaknesses and action plans
  * Maturity audit report

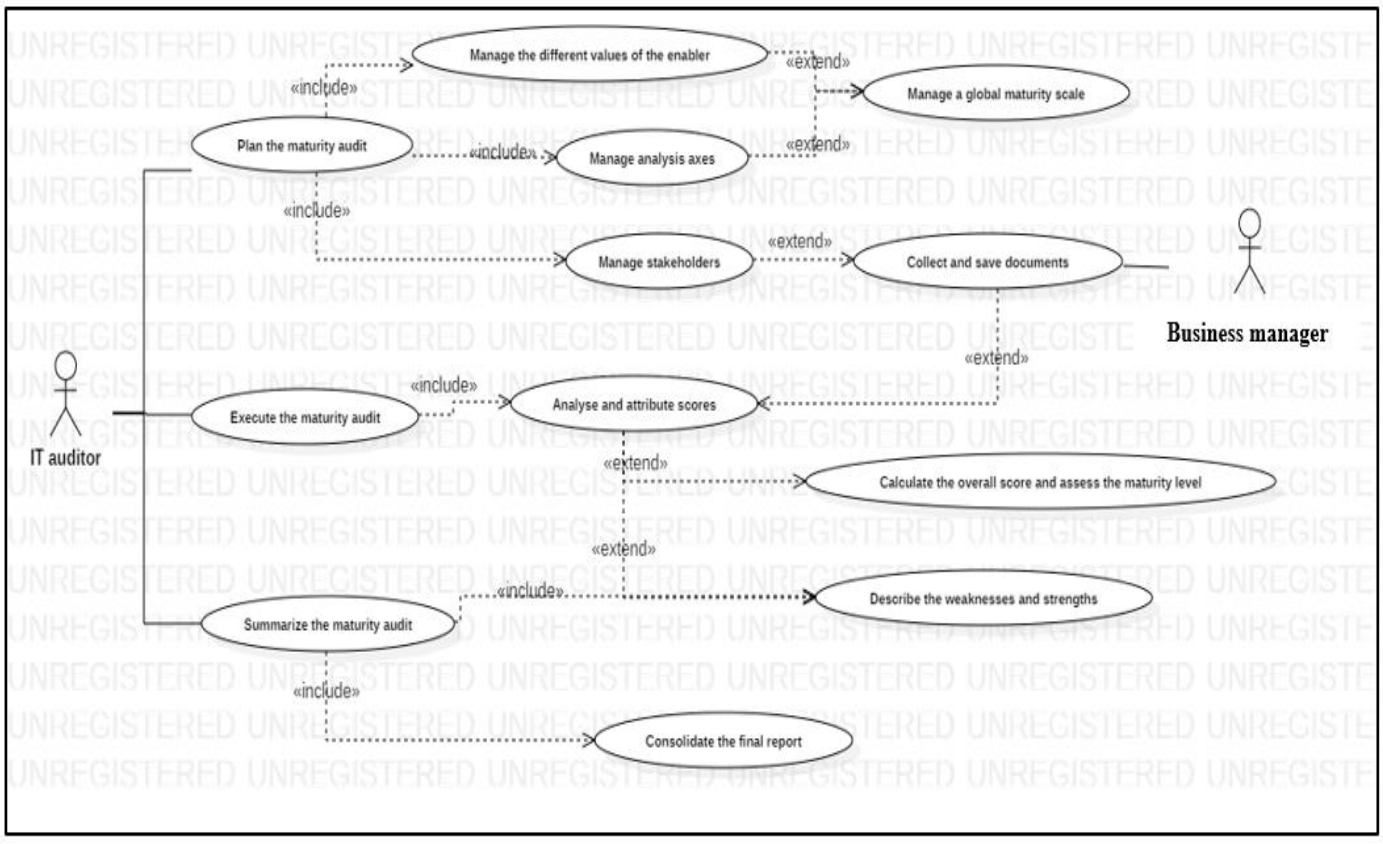


Figure 4. Use case diagram detailing features of MART 23 (designed with the test version of StarUML software)

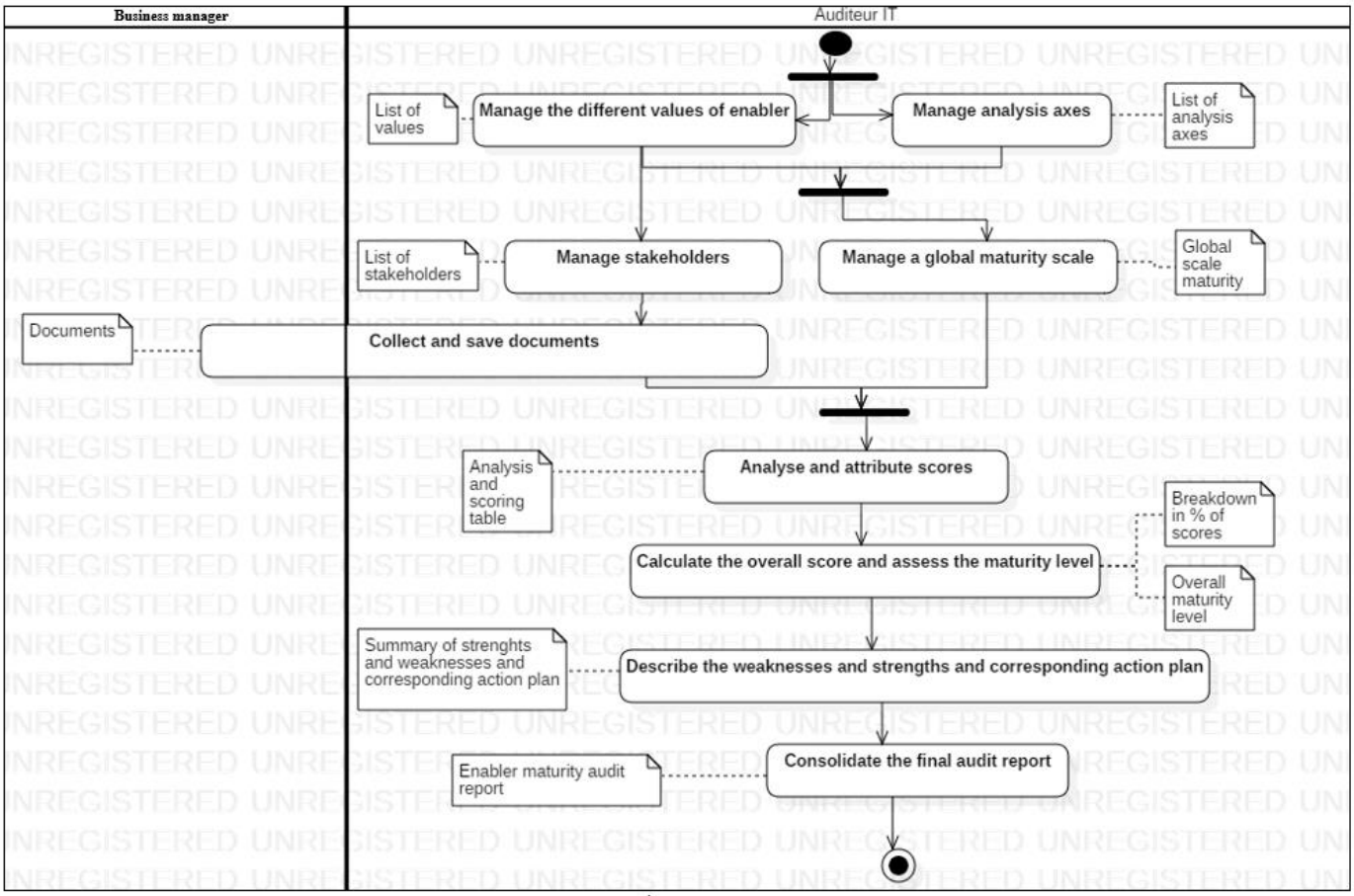


Figure 5. Activity diagram to describe the flow of activities corresponding to each use case of MART 23 (designed with the test version of StarUML software)

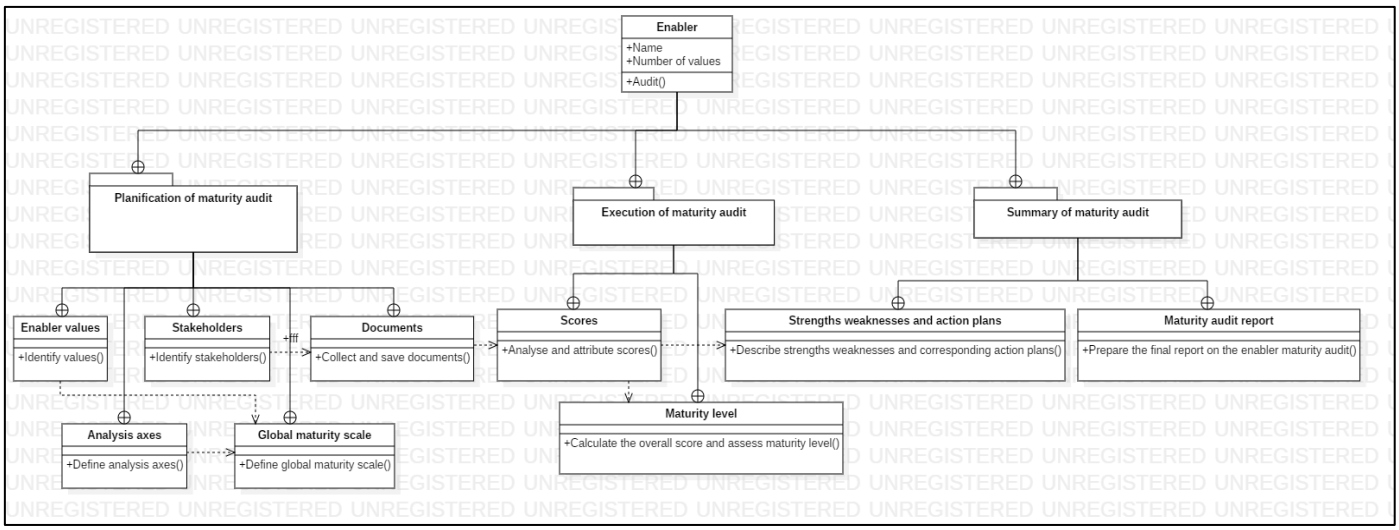


Figure 6. Class diagram to describe classes, structure and associations of MART 23 (designed with the test version of StarUML software)

3.2 Development of MART 23

Following the design, we will proceed with the development of the system MART 23 via a web application. For system development, we opted for an MVC architecture (Model, View, Controller) to better organize our system's source code. The backend was developed by Java, the most dominant language for developing computer applications, especially web applications, and the frontend was developed using Typescript. This language improves and secures the development of JavaScript-compatible code. In terms of frameworks, we mainly used: Springboot (a JAVA development framework based on Spring) and Angular (a development framework based on TypeScript and using an MVC architecture). Regarding the database, MySQL has been chosen as the relational database server.

The aim of this section is to present some of the graphical layouts of the system MART 23:

3.2.1 Home pages

The MART 23 system has been developed to enable any organization to probe the maturity of its ITRM. In this sense, the system can be used either by an organization that has already carried out the audit previously, or by a new organization wishing to launch its first ITRM maturity audit. The interface shown in Figure 7 invites the user to choose between a new or an existing institution.

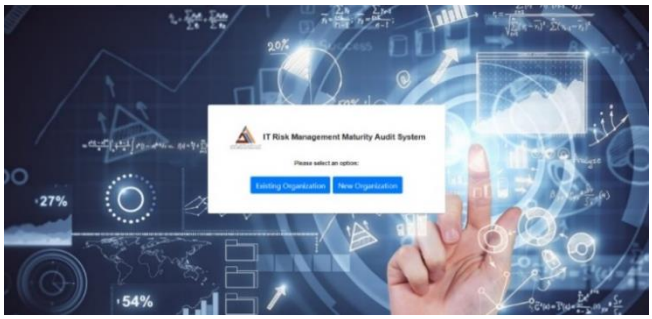


Figure 7. Choosing between a new or existing institution

When the "new organization" button is clicked, the interface shown in Figure 8 appears, asking the user to enter the name of the organization. When the user clicks on next, this name is automatically saved in the database.

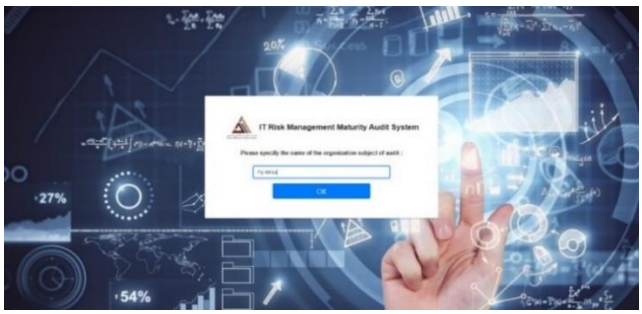


Figure 8. Insert organization name

Clicking on "next" takes you to the Home page (Figure 9), showing the 7 maturity audit axes.

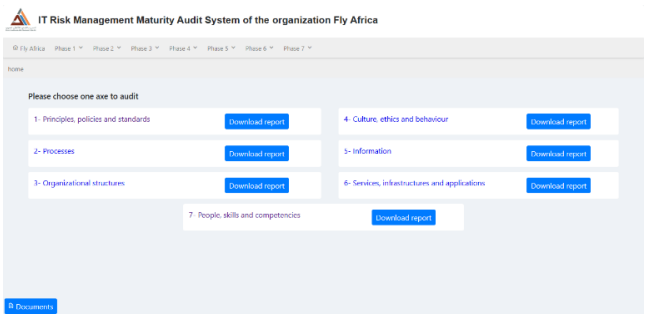


Figure 9. Home page

The user can choose to start with any audit axis, and we assume that the selected choice is the maturity audit of principles, policies and frameworks.

3.2.2 Step 1 – Setting up the audit of maturity of "Principles, policies and frameworks" in relation with ITRM

The first stage of the maturity audit project consists of defining the various parameters required for the audit, in particular:

- Choice of IT risk management principles. By default, all principles are deactivated, and the IT auditor can select those not applicable to the organization to be audited.
- Choice of IT risk management policies. By default, all policies are disabled, and the IT auditor can select policies not applicable to the organization to be audited (Figure 10).

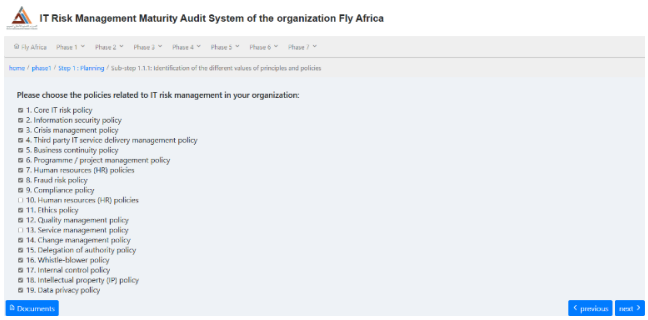


Figure 10. Choice of policies to be audited

- Choice of analysis axes to be applied. By default, all analysis axes are selected, but the IT auditor can deselect analysis axes that are not applicable to the organization to be audited, explaining the reasons for the deselection (Figure 11).

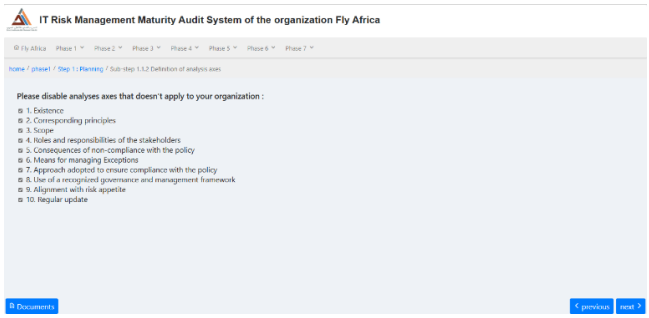


Figure 11. Choosing the axes of analysis to be used for the audit

- Definition of the maturity scale. Depending on the number of analysis axes and policies selected, a maturity scale is calculated and displayed by default (Figure 12). The IT auditor has the choice of changing the intervals of each maturity level according to the needs of the organization to be audited, while respecting certain management rules implemented in the system, namely:

  * Maturity level 0 is unchangeable.
  * The minimum of maturity level 1 and the maximum of maturity level 5 are fixed and remain unchangeable.
  * The intervals of the different levels follow one another and change automatically by changing one of the values.

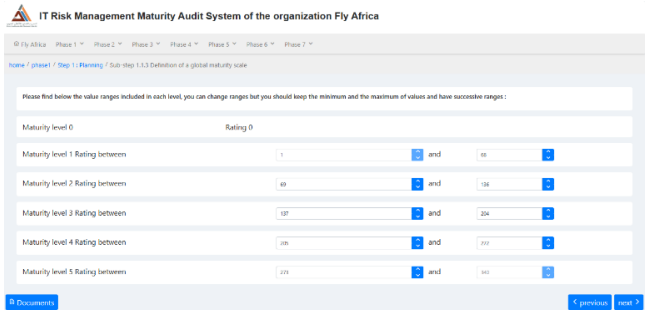


Figure 12. Maturity scale

- Identification of the various stakeholders required for the audit. The internal auditor can add, delete or modify each stakeholder.

- Upload the documents required for the audit. The IT auditor has the option of loading or deleting documents as required during all stages of the project, by accessing them via the "Documents" button (Figure 13).

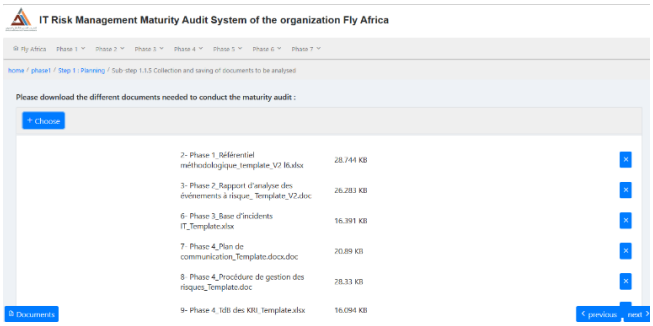


Figure 13. Document loading page

3.2.3 Step 2 - Execution of the audit of maturity of "Principles, policies and frameworks" in relation with ITRM

The second stage of the maturity audit project is to carry out a maturity audit of the various policies applicable to the organization and according to the previously selected analysis axes, assigning each cell in the table shown in Figure 14 a score of 0, 1 or 2. The maturity audit is based on the analysis of the documents collected previously, and by questioning the stakeholders concerned. The IT auditor is the only person with access to the system, to secure the audit results.

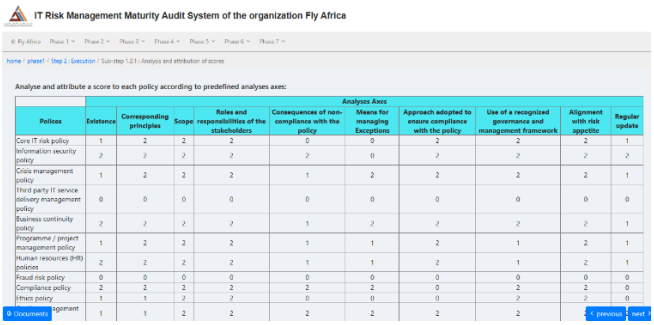


Figure 14. Audit scoring table

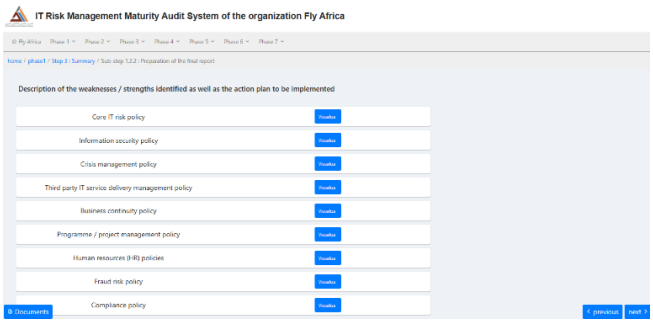


Figure 15. List of policies applicable to the audited organization

3.2.4 Step 3 - Summary of the audit of maturity of "Principles, policies and frameworks" in relation with ITRM

Following the assignment of scores in step 2 of auditing the maturity, it is possible in step 3 to display a summary of the score for each policy. As shown in Figure 15, the list of policies applicable to the audited organization is displayed. To view the rating details for each policy, press the "Visualize" button. This produces a radar (Figure 16) displaying the different axes of analysis and the score attributed to each axis, as well as an action plan to be deployed to improve the maturity of the policy displayed.

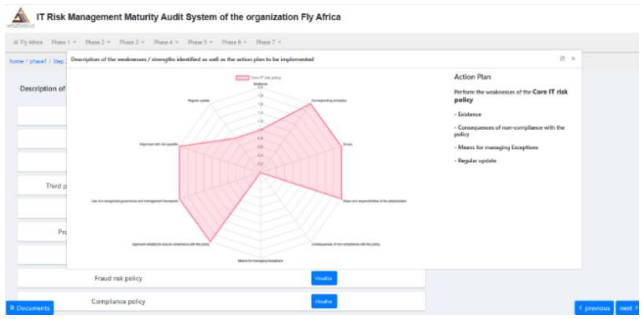


Figure 16. Core IT risk policy maturity audit radar

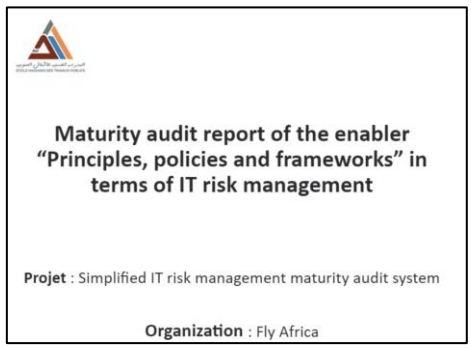


Figure 17. Extract of the reporting about auditing the maturity - Front page

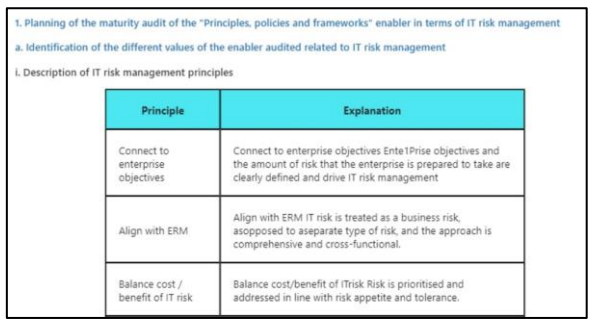


Figure 18. Extract of the reporting about auditing the maturity - Description of ITRM principles

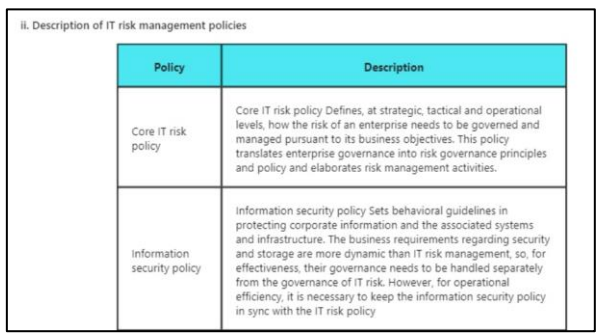
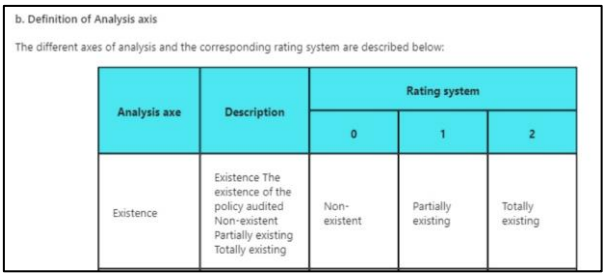


Figure 19. Extract of the reporting about auditing the maturity - Description of ITRM policies

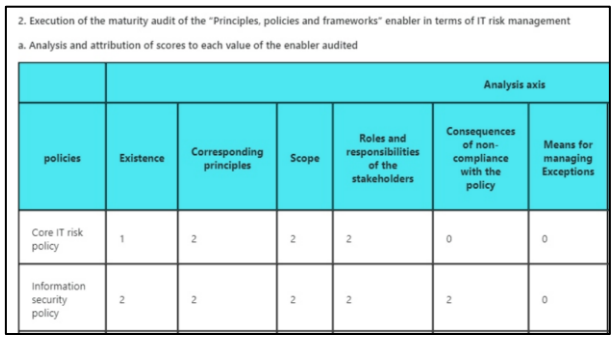


b. Definition of Analysis axis

The different axes of analysis and the corresponding rating system are described below:

Analysis axe	Description	Rating system		
		0	1	2
Existence	Existence The existence of the policy audited Non-existent Partially existing Totally existing	Non-existent	Partially existing	Totally existing

Figure 20. Extract of the reporting about auditing the maturity - Definition of analysis axes

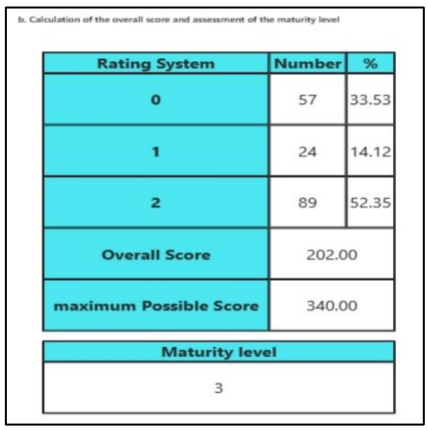


2. Execution of the maturity audit of the "Principles, policies and frameworks" enabler in terms of IT risk management

a. Analysis and attribution of scores to each value of the enabler audited

	Analysis axis					
policies	Existence	Corresponding principles	Scope	Roles and responsibilities of the stakeholders	Consequences of non-compliance with the policy	Means for managing Exceptions
Core IT risk policy	1	2	2	2	0	0
Information security policy	2	2	2	2	2	0

Figure 21. Extract of the reporting about auditing the maturity - Analysis and attribution of scores



b. Calculation of the overall score and assessment of the maturity level

Rating System	Number	%
0	57	33.53
1	24	14.12
2	89	52.35
Overall Score	202.00	
maximum Possible Score	340.00	

Maturity level
3

Figure 22. Extract of the reporting about auditing the maturity - Calculation of the total score and evaluation of the maturity level

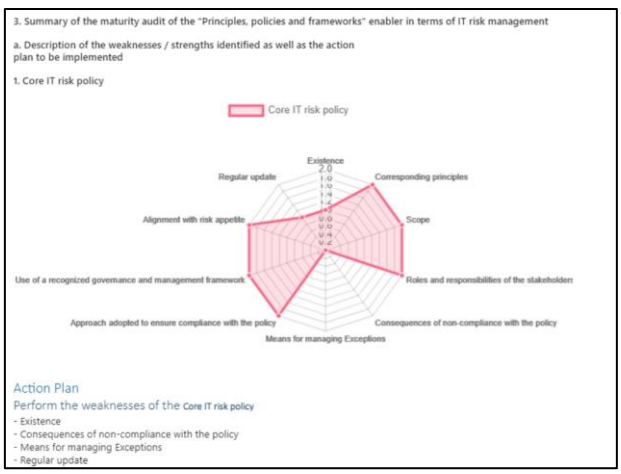


Figure 23. Extract of the reporting about auditing the maturity - Core IT risk policy maturity audit radar

Clicking on "next" takes you to the reporting about auditing the maturity of the enabler "Principles, policies and frameworks". Figures 17-23 show extracts from this report.

4. CONCLUSION & PERSPECTIVES

In this article, we have presented the system MART 23 used to audit the maturity of ITRM within organizations. The system was created by using a methodological approach built on guidelines of COBIT 5. We started by a remind of the methodological approach detailed in a previous article. Then we proceeded to the design of the system using UML. We presented context, use case, activity and class diagrams. After that, we developed the system using JAVA language and presented some layouts of that system. The application of the MART 23 system within organizations will allow these last to improve the maturity level of managing information technology risks by implementing the action plans described in the final maturity audit report.

For next steps, the MART 23 system should be validated using case studies from organizations in different sectors. Besides, the design of the reports generated could be improved by using specialized reporting tools.

REFERENCES

[1] IBM, Méthodologie de gestion du risque informatique pour les Directeurs des Systèmes d'Information: Un levier exceptionnel de création de valeur et de croissance, 2008. https://dokumen.tips/documents/5716-gben-prf-ibmcom-du-fait-de-lomnipresence-de-linformatique-dans.html?page=2.

[2] Amansou, S. (2019). Gestion des risques: Fondements théoriques et analyse critique. Assurances et Gestion des Risques, 86(2-3): 265-287. https://doi.org/10.7202/1068509ar

[3] 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

[4] Ernawati, T., Suhardi, Nugroho, D.R. (2012). IT risk management framework based on ISO 31000:2009. In 2012 International Conference on System Engineering and Technology (ICSET), Bandung, Indonesia. https://doi.org/10.1109/ICSEngT.2012.6339352

[5] 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

[6] COSO. (2013). Internal control - integrated framework. https://www.coso.org/guidance-on-ic, accessed on Aug. 6, 2023.

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

[8] COSO. (2017). Enterprise risk management - integrating with strategy and performance. https://aaahq.org/portals/0/documents/coso/coso_erm_2017_main_v1_20230815.pdf, accessed on Sep. 4, 2023.

[9] ISO, ISO 31000 - Management du risque, ISO Publication, 2018. https://www.iso.org/fr/standard/65694.html#:~:text=Qu'est%2Dce%20qu',et%20communiquer%20sur%20ces%20derniers.

[10] G. Sutra, Management des risques: Une approche stratégique, Afnor Editions, 2018. https://scholar.google.com/scholar_lookup?title=Management%20des%20risques:%20une%20approche%20strat%C3%A9gique&publication_year=2018&author=G.%20Sutra

[11] ISACA, COBIT 5: A business framework for Governance and Management of enterprise IT, USA: ISACA Publication, 2012. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0.

[12] ISACA, Relating the Coso internal control - integrated framework and Cobit, Isaca Cobit series white paper, 2014. https://informationsecurity.report/Resources/Whitepapers/f9d00ce2-f760-4be5-bdd8-fa44371493b7_Relating-the-COSO-Internal-Control-Integrated-Framework-and-COBIT_whp_Eng_0314.pdf.

[13] ISACA, COBIT 5 for Risk, USA: ISACA Publication, 2013. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoAmEAK.

[14] Kozina, M. (2021). IT risk management in the enterprise using CobiT 5. In Proceedings of the Central European Conference on Information and Intelligent Systems, Varaždin, Croatia, pp. 249-256. https://scholar.google.com/scholar?cluster=7788059389304324409&hl=fr&as_sdt=2005&sciodt=0,5.

[15] 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. https://doi.org/10.1109/InfoSec.2015.7435520

[16] Berrada, H., Boutahar, J., El Ghazi El Houssaïni, S. (2023). Roadmap and information system to implement information technology risk management. International Journal of Safety and Security Engineering, 13(6): 987-1000. https://doi.org/10.18280/ijsse.130602

[17] Berrada, H., El Ghazi El Houssaïni, S., Boutahar, J. (2023). Implementing information technology risk management: A case study in the African airline industry. Journal of Organizations, Technology and Entrepreneurship, 1(1): 58-76. https://doi.org/10.56578/jote010105

[18] Berrada, H., Boutahar, J., El Houssaïni, S.E.G. (2023). RITM 23: A system to an IT risk management implementation. In 2023 3rd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Mohammedia, Morocco, pp. 1-6. http://doi.org/10.1109/iraset57153.2023.10152978

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

[20] ISACA, COBIT 5: Enabling Processes, USA: ISACA Publication, 2012. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCIEA0.