Simplified IT Risk Management Maturity Audit System based on “COBIT 5 for Risk”

Hasnaa Berrada, Jaouad Boutahar, Souhaïl El Ghazi El Houssaïni
Systems, Architectures and Networks Team, EHTP
Casablanca, Morocco

***Abstract*—In recent years, the role of risk management has emerged as a key success factor in ensuring the growth on the one hand and the survival on the other hand of any organization. Moreover, dependence on IT has become systematic within any organization. This dependence therefore, implies the importance of implementation of an IT risk management system in order to well manage IT risks. There are several standards that deal with enterprise risk management in general or information security in particular. However, few standards deal with IT risk management. Noting, for example, COBIT 5 (Control Objectives for Information and related Technology) which deals with IT risk management but is complicated to deploy. The purpose of this article is to describe a simplified IT risk management maturity audit system in an organization based on “COBIT 5 for risk”. This system aims to evaluate the maturity of IT risk management before proceeding to the implementation or update of an IT risk management system within an organisation.**

Keywords—IT risk management; COBIT 5 for risk; maturity audit system; COBIT 5 enablers; analysis axes; maturity scale and score; maturity audit report

I. Introduction

Taking risks is a prerequisite for the survival and growth of any business. By consequence, it is essential to properly manage and control the risks inherent in the activity, otherwise, if these risks arise, the company will not be able to achieve its objectives [1] [2].

On the other hand, with the emergence of Information Technology, which has become an integral part of any business ecosystem, IT risk management is becoming vital for the business [3].

“Risk management is a process that aims to reduce the harmful effects of an activity through conscious action to anticipate unwanted events and plan to avoid them. Risk management can be thought a process of measuring or evaluating risk and then designing strategies for risk management” [4] [5] [6] [7].

Therefore, standards have been developed to deal with risk management in general, IT risk management and information security in particular. Many risk management standards or information security standards exist, but few are the standards that deal with the question of IT risk management.

Noting for example, COSO, an internal control reference framework developed by the Committee of Sponsoring Organizations of the Treadway Commission and aims to improve the performance and governance of companies as well as reduce fraud within organizations [8].

On the other hand, there is the COBIT, a reference framework for IT audit and IT governance, is intended for management (which must decide on the investments to be made, to ensure the security and control of IT, and adjust them according to the risks of the environment) and the users (security, control of the IT services provided) [9] [10].

The COBIT 5 framework includes specific documentation for IT risk management called “COBIT 5 for Risk [11]” but this framework is complicated to deploy with a large library of publications requiring operationalization and consolidation of concepts related to IT risk management.

To respond to these limitations, we had focused our research on the development of a simplified IT risk management system that can be used easily within an organization. The first step in this development starts with the setting up of an IT risk management maturity audit system. The main purpose of this system is to evaluate the maturity of IT risk management, identify the gaps and define action plans that will allow the setting up or update of IT risk management within an organization. In this article we’ll describe a proposed system for IT risk management maturity audit within an organization based on “COBIT 5 for Risk”.

After an introduction, we will present a review of the literature on IT risk management. The next part will describe the methodological approach to be adopted when setting up the maturity audit system for the IT risk management of an organization. Afterwards, we will describe the proposed system for the maturity audit of the IT risk management of an organization. We will end with a conclusion and perspectives.

II. Review of the Literature on IT Risk Management

A risk can be defined as the “effect of uncertainty on objectives. An effect is a deviation from the expected - positive or negative. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.” [12] [13].

“COBIT 5 for Risk defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT risk consists of IT-related events that could potentially impact the business. IT risk can occur with both uncertain frequency and impact and creates challenges in meeting strategic goals and objectives.” [11].

Risk management is the “coordinated activities to direct and control an organization with regard to risk”. As a consequence, risk management framework is a “set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.” [13].

Within the framework of risk management, several standards exist. Noting, for example, the COSO, a reference framework for internal control developed by the Committee Of Sponsoring Organizations of the Treadway Commission and aimed at improving the performance and governance of companies as well as reducing fraud within organizations. [8].

On the other hand, there is the COBIT which constitutes a reference framework for IT audit and IS governance and which is intended for both management and users. This framework includes dedicated documentation for IT risk management: “COBIT 5 For Risk” [11].

Regarding ISO 31000, it is a standard that provides principles and guidelines for risk management as well as the implementation processes at the strategic and operational level [14].

For ISO / IEC 27005, it is a standard that describes the main lines of risk management with a view to setting up an information security management system [15].

Below is a comparative table of a selection of existing standards related to risk management (Table I):

TABLE I. COMPARATIVE TABLE OF RISK MANAGEMENT FRAMEWORKS / STANDARDS

Framework / standard	**Enterprise Risk Management Framework / standard**	**IT Risk Management Framework / standard Framework**	**Information Security Risk Management Framework / standard k Management Framework / standard**
COSO	✓	×	×
ISO 31000	✓	×	×
ISO/CEI 27005	×	×	✓
COBIT 5	×	✓	×

Except COBIT 5, all of the frameworks / standards are either generic risk management frameworks, or specific frameworks for information security risk management and do not deal with all components of IT risk management. The COBIT 5 framework includes specific documentation for IT risk management called “COBIT 5 for Risk” but this framework is complicated to deploy with a large library of publications requiring operationalization and consolidation of concepts relating to IT risk management.

In addition, the COBIT 5 is a framework that aligns and incorporates the key components of other risk management frameworks [11] [10]:

- ISO 31000 (principles, Risk management Framework, process for managing risk).
- ISO/IEC 27005 (process).
- COSO (components, principles).

In the literature, there are research articles that discuss the COBIT 5 deployment for IT risk management. Authors “Walid Al-Ahmad” and “Basil Mohammed” in their article [16] present the business processes used in information security risk management, as well as the corresponding activities and guidelines for implementing them. This article does not take into account IT risk governance processes (EDM03 Ensuring risk optimization) and focuses on information security risk management. The authors “Hanim Maria Astuti et al.” in their article [17] present a case study for the COBIT 5 deployment for the identification, assessment and management of IT risks of an organizational unit (Service Desk). This article is limited to the deployment of the two COBIT 5 processes: DSS02 Manage service and APO12 Manage Risks.

The main limitation noted of the two research articles cited above is that they partially cover the implementation of an IT risk management system and do not detail the IT risk governance process.

According to the different elements mentioned above, a research work has been launched for the development of an IT risk management system based on COBIT 5. This article presents the first phase of the development of this system and which consists of the description of a maturity audit system of the IT risk management of an organization.

III. DESCRIPTION OF THE METHODOLOGICAL APPROACH TO BE ADOPTED

In order to setting up a maturity audit system IT risk management within an organization, we suggest adopting an approach based on the analysis of the Risk Function perspective described by COBIT 5 for risk (Fig. 1). The Risk Function Perspective “describes what is necessary in a company to effectively and efficiently build and maintain governance and risk management activities”. [11].

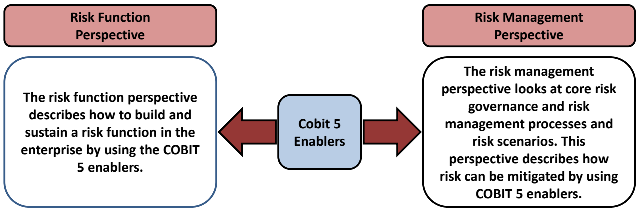

Risk Function Perspective
The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.
Cobit 5 Enablers
Risk Management Perspective
The risk management perspective looks at core risk governance and risk management processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

Fig. 1. The Two perspectives of Risk Proposed by COBIT 5 [11].

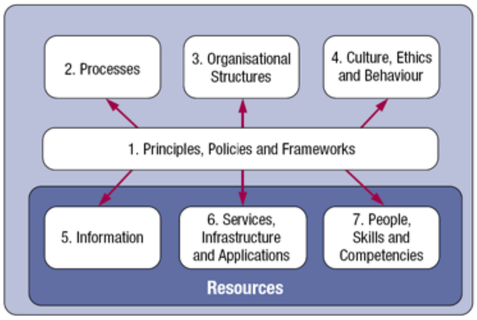

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Fig. 2. The Seven COBIT 5 Enablers [9].

Indeed, the risk function perspective is based on the seven COBIT 5 enablers (Fig. 2) [9] in order to detail the different functions / dimensions of an organization that enable IT risk governance and management. An enabler can be considered as a dimension or a pillar for the establishment of IT governance.

The proposed methodological approach is broken down into seven macro-phases in alignment with the seven enablers defined by COBIT 5 (Table II.):

TABLE II. THE 7 MACRO-PHASES OF THE METHODOLOGICAL APPROACH TO BE ADOPTED FOR THE MATURITY AUDIT OF IT RISK MANAGEMENT WITHIN AN ORGANIZATION

Macro phase 1	Maturity audit of principles, policies and standards related to IT risk management
Macro phase 2	Maturity audit of IT risk management processes
Macro phase 3	Maturity audit of organizational structures related to IT risk management
Macro phase 4	Maturity audit of culture, ethics and behaviour related to IT risk management
Macro phase 5	Maturity audit of information related to IT risk management
Macro phase 6	Maturity audit of services, infrastructures and applications related to IT risk management
Macro phase 7	Maturity audit of people, skills and competencies related to IT risk management

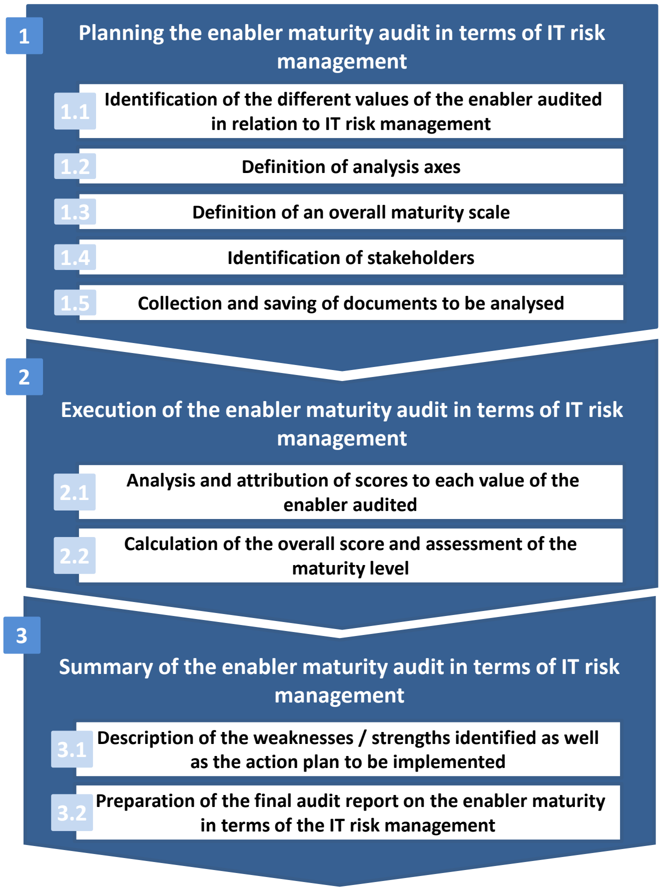

1
Planning the enabler maturity audit in terms of IT risk management
1.1
Identification of the different values of the enabler audited in relation to IT risk management
1.2
Definition of analysis axes
1.3
Definition of an overall maturity scale
1.4
Identification of stakeholders
1.5
Collection and saving of documents to be analysed
2
Execution of the enabler maturity audit in terms of IT risk management
2.1
Analysis and attribution of scores to each value of the enabler audited
2.2
Calculation of the overall score and assessment of the maturity level
3
Summary of the enabler maturity audit in terms of IT risk management
3.1
Description of the weaknesses / strengths identified as well as the action plan to be implemented
3.2
Preparation of the final audit report on the enabler maturity in terms of the IT risk management

Fig. 3. Methodological Approach to be adopted to Audit IT Risk Management Maturity.

For each macro-phase, all of the steps described in Fig. 3 must be taken to audit the level of maturity of each enabler (Except the "Process" enabler whose maturity audit steps are partially described by the COBIT 5 [9]) in terms of IT risk management:

Step 1: Planning the enabler maturity audit in terms of IT risk management

Sub-step 1.1: Identification of the different values of the enabler audited in relation to IT risk management

For each enabler, the objective is to define its different values in relation to IT risk management in order to audit each value according to the defined axes of analysis.

Delivery: List of values of the enabler audited.

Sub-step 1.2: Definition of analysis axes

For each enabler, a set of good practices to be observed are specified by COBIT 5, on the basis of these good practices, the different axes of analysis are defined.

Delivery: List of axes of analysis.

Sub-step 1.3: Definition of an overall maturity scale

The maturity scale varies between 1 and 5. The definition of the value ranges included in each level is defined according to the minimum score and the maximum score of the enabler being audited.

Delivery: Global maturity scale.

Sub-step 1.4: Identification of stakeholders

We determine the various stakeholders necessary for the conduct of the enabler maturity audit in terms of IT risk management. For each value of the enabler audited, we define the business manager who will collaborate with the IT auditor in order to carry out the audit.

Delivery**:** List of stakeholders.

Sub-step 1.5: Collection and saving of documents to be analysed

We collect and save the various documents to be analysed in order to audit the maturity of the IT risk management of the facilitator being audited.

Delivery**:** Documents to analyse

Step 2: Execution of the enabler maturity audit in terms of IT risk management

Sub-step 2.1: Analysis and attribution of scores to each value of the enabler audited

We analyze each value of the enabler audited and assign a score per axis of analysis.

Delivery: Analysis and scoring table of the audited enabler.

Sub-step 2.2: Calculation of the overall score and assessment of the maturity level

We calculate the number and the percentage of the different scores assigned by axis of analysis and by value of the enabler audited (the number and the percentage of 0, 1 and 2). The overall score is calculated by summing all the scores. Depending on the overall score obtained, a maturity level is obtained in accordance with the previously defined maturity scale.

Delivery: Breakdown in percentage of scores 0, 1 and 2,

Overall maturity level of the enabler audited.

<u>Step 3: Summary of the enabler maturity audit in terms of IT risk management</u>

<u>Sub-step 3.1: Description of the weaknesses / strengths identified as well as the action plan to be implemented</u>

Based on the analysis of each value of the enabler according to the predefined axes of analysis, the strengths and weaknesses are identified as well as the action plan to be implemented to remedy the weaknesses observed.

Delivery: Summary of strengths and weaknesses and corresponding action plan.

<u>Sub-step 3.2: Preparation of the final audit report on the enabler maturity in terms of the IT risk management</u>

Prepare the maturity audit report for the enabler in terms of IT risk management, including a description of the various stages carried out and the audit results obtained.

Delivery: Enabler maturity audit report in terms of IT risk management.

IV. Description of the Proposed Simplified IT Risk Management Maturity Audit System

In this part, we will describe the simplified IT risk management maturity audit system in an organization by reviewing the different macro-phases. The first two macro-phases (Table II) will be described in detail; the others are similar to the first macro-phase except for certain steps which will be described below.

A. *Maturity audit of the Principles, Policies and Frameworks Related to IT Risk Management*

1) Planning of the maturity audit of the "Principles, policies and frameworks" enabler in terms of IT risk management

a) Identification of the different values of the enabler audited related to IT risk management

This step consists in identifying the principles and policies making it possible to build and implement IT risk management in an organization.

COBIT 5 defines seven principles in relation to IT risk management (Fig. 4) [18].

Regarding policies, COBIT 5 lists 18 policies with the description of each policy. Below are the 18 policies mentioned by COBIT 5 (Fig. 5) [11].

b) Definition of analysis axes: This step consists in determining the analysis axes based on the good practices of COBIT 5 [11]. The different axes of analysis and the corresponding rating system are described (Table III).

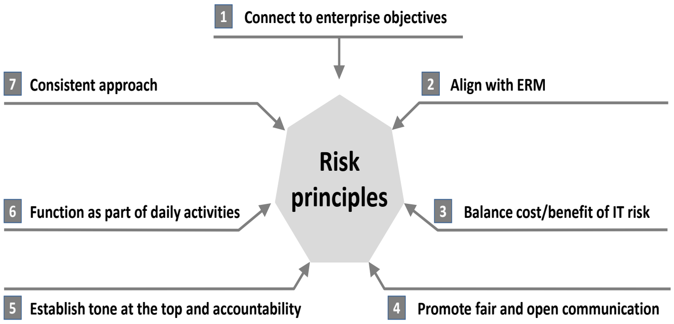
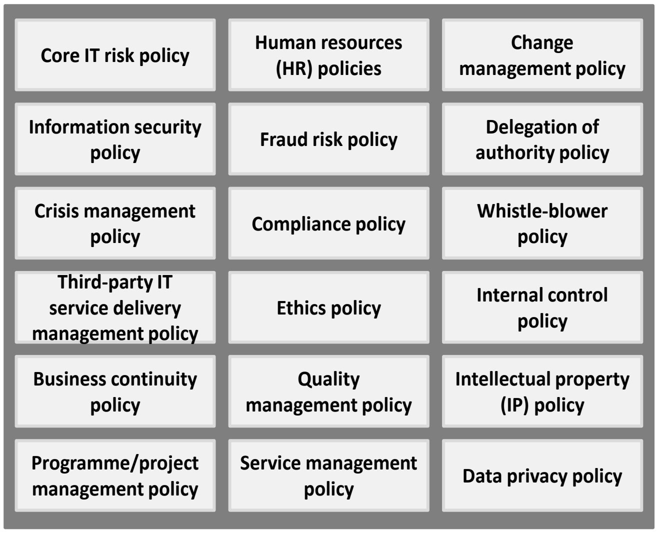

1 Connect to enterprise objectives
7 Consistent approach
2 Align with ERM
Risk principles
6 Function as part of daily activities
3 Balance cost/benefit of IT risk
5 Establish tone at the top and accountability
4 Promote fair and open communication

Fig. 4. Principles of Risk Management.



Core IT risk policy	Human resources (HR) policies	Change management policy
Information security policy	Fraud risk policy	Delegation of authority policy
Crisis management policy	Compliance policy	Whistle-blower policy
Third-party IT service delivery management policy	Ethics policy	Internal control policy
Business continuity policy	Quality management policy	Intellectual property (IP) policy
Programme/project management policy	Service management policy	Data privacy policy

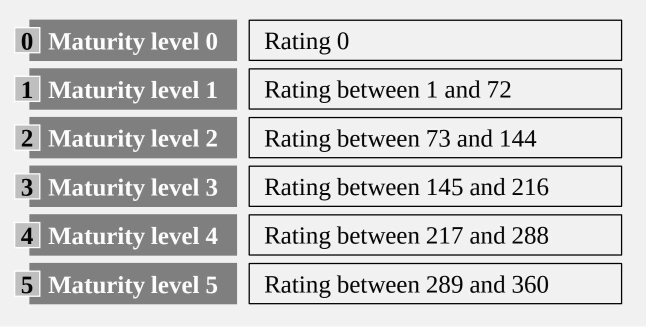
Fig. 5. The 18 Policies Defined by COBIT 5.

TABLE III. ANALYSIS AXES THE ENABLER "PRINCIPLES, POLICIES AND FRAMEWORKS"

Analysis axe	Description	Rating system		
		0	1	2
Existence	The existence of the policy audited	Non-existent	Partially existing	Totally existing
Corresponding principles	Correspondence between each policy and the 7 principles retained by COBIT 5	No principle corresponds to the policy to be audited	The policy to be audited corresponds to 1 or 2 or 3 principles	The policy to be audited corresponds to 4 or more principles
Scope	Description of the scope of application of the audited policy	Non-existent	Partially existing	Totally existing
Roles and responsibilities of the stakeholders	Description of the roles and responsibilities of the stakeholders of the audited policy	Non-existent	Partially existing	Totally existing
Consequences of non-compliance with the policy	Description of the consequences of non-compliance with the policy audited	Non-existent	Partially existing	Totally existing
Means for managing exceptions	Description of the means to be deployed to manage exceptions to the audited policy (for example: disciplinary measures, warning, etc.)	Non-existent	Partially existing	Totally existing
Approach adopted to ensure compliance with the policy	Description of the approach adopted to ensure compliance with the audited policy	Non-existent	Partially existing	Totally existing
Use of a recognized governance and management framework	The use of a recognized governance and management framework for the definition of the audited policy	No	Partially	Yes
Alignment with risk appetite	Alignment of the audited policy with the risk appetite determined by the organization	No	Partially	Yes
Regular update	The regularity of updating the audited policy	No	Partially	Yes

c) Definition of a global maturity scale

In this step, we define a maturity scale that varies between 0 and 5 and is divided between the minimum score and the maximum score (Fig. 6):



0	Maturity level 0	Rating 0
1	Maturity level 1	Rating between 1 and 72
2	Maturity level 2	Rating between 73 and 144
3	Maturity level 3	Rating between 145 and 216
4	Maturity level 4	Rating between 217 and 288
5	Maturity level 5	Rating between 289 and 360

Fig. 6. Global Maturity Scale of the Enabler "Principles, Policies and Frameworks".

d) Identification of stakeholders

In this step, we determine the various stakeholders necessary for the conduct of the maturity audit process of the macro-phase "maturity audit of principles, policies and frameworks related to IT risk management". For each policy, we define the business manager who will coordinate with the IT auditor in order to carry out the audit.

e) Collection and saving of documents to be analysed

In this step, we collect and save the various existing policies in order to analyze them and audit the maturity of the IT risk management of the "Principles, Policies and Frameworks" enabler.

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

In this step, we analyze each policy according to the predefined analysis axes and we attribute a score per axe according to predefined rating system (Table IV):

TABLE IV. ANALYSIS AND ATTRIBUTION OF SCORES TO EACH POLICY ACCORDING TO PREDEFINED ANALYSIS AXES AND RATING SYSTEM

Policy	***Core IT risk policy***	***Third party IT service delivery management policy***
Existence	1	1
Corresponding principles	2	2
Scope	1	0
Roles and responsibilities	1	1
Consequences of non-compliance	1	0
Means for managing exceptions	1	1
Approach adopted to ensure compliance with the policy	1	1
Use of a recognized governance and management framework	1	0
Alignment with risk appetite	1	1
Regular update	1	0

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

This step consists in calculating the number and the percentage of the different possible scores (0, 1 and 2). Then calculating the overall score by summing all the scores awarded by value of the enabler and by analysis axe. The overall score makes it possible to assess the level of maturity of policies, principles and frameworks according to the positioning in the global maturity scale.

3) Summary of the maturity audit of the "Principles, policies and frameworks" enabler in terms of IT risk management.

a) Description of the weaknesses / strengths identified as well as the action plan to be implemented.

This step consists of positioning for each policy audited the scores assigned by analysis axe on a radar to better identify the strengths and weaknesses (Fig. 7).

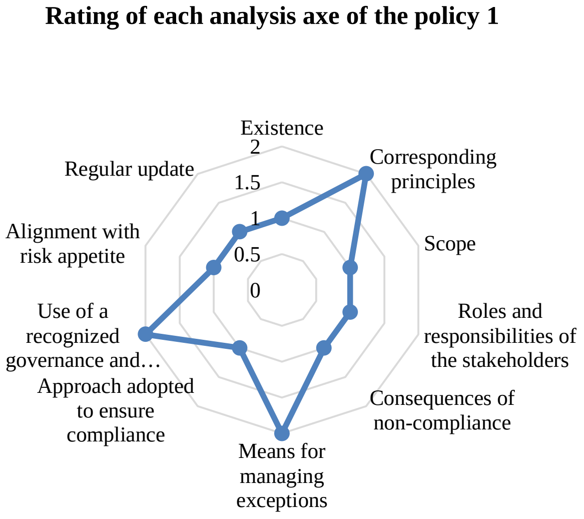


Fig. 7. Graphical Representation of Ratings Assigned to Policy 1.

Then, we proceed to the description of the strengths / weaknesses identified of each policy and we propose the action plans to be implemented to improve the level of maturity of the "Principles, Policies and Frameworks" enabler.

b) Preparation of the final report on the enabler maturity audit in terms of IT risk management.

In this step, the maturity audit report of the enabler "Principles, policies and frameworks" in terms of IT risk management is drawn up, with a description of the various stages carried out and the audit results obtained.

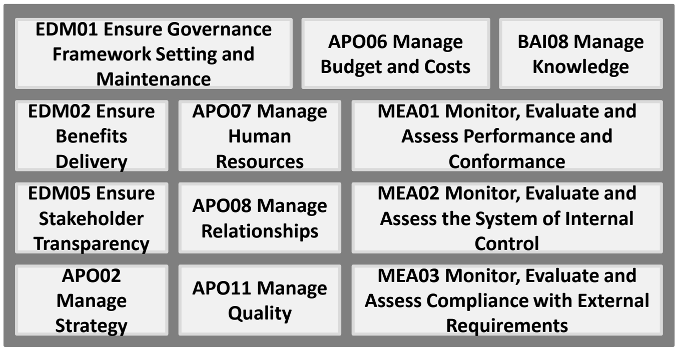
B. Maturity Audit of IT Risk Management Processes

The first step is to identify the processes needed for building and implementing IT risk management in an organization.

COBIT 5 defines 2 core processes dedicated only for IT risk governance and management [11] [19]:

- EDM03 Ensure Risk Optimization
- APO12 Manage Risk

COBIT 5 defines 12 supporting processes for IT risk governance and management (Fig. 8) [11] [19]:



EDM01 Ensure Governance Framework Setting and Maintenance

APO06 Manage Budget and Costs

BAI08 Manage Knowledge

EDM02 Ensure Benefits Delivery

APO07 Manage Human Resources

MEA01 Monitor, Evaluate and Assess Performance and Conformance

EDM05 Ensure Stakeholder Transparency

APO08 Manage Relationships

MEA02 Monitor, Evaluate and Assess the System of Internal Control

APO02 Manage Strategy

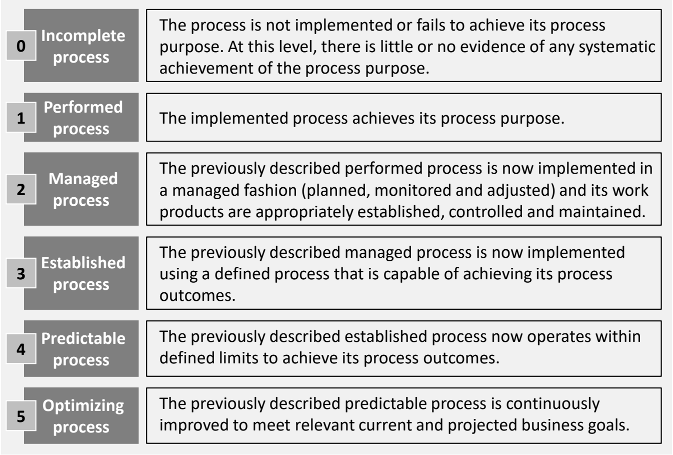
APO11 Manage Quality

MEA03 Monitor, Evaluate and Assess Compliance with External Requirements

Fig. 8. Supporting Processes for IT Risk Governance and Management.

The rest of the 23 processes defined by COBIT 5 [19] also help in governance and IT risk management, but the contribution is low. These processes will therefore not be subject to a maturity audit.

The second step consists in determining the analysis axes, we retain the level of maturity of the process according to the maturity scale defined by COBIT 5. The level of maturity makes it possible to audit the maturity of a process, 6 maturity levels are defined in COBIT 5 (Fig. 9) [9]:



0	Incomplete process	The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
1	Performed process	The implemented process achieves its process purpose.
2	Managed process	The previously described performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
3	Established process	The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes.
4	Predictable process	The previously described established process now operates within defined limits to achieve its process outcomes.
5	Optimizing process	The previously described predictable process is continuously improved to meet relevant current and projected business goals.

Fig. 9. Maturity Scale of Processes Defined by COBIT 5.

In the third step, we determine the different stakeholders necessary for the conduct of the process maturity audit. For each process, we define the business manager who will coordinate with the IT auditor to carry out the audit.

In the fourth step, we collect and save the documentation relating to existing processes in order to analyze and audit the maturity of the IT risk management of the "Process" enabler.

In the fifth step, we assess the maturity level of each process defined in the first step.

In the sixth step, the overall score is calculated by applying the following formula (1):

$$N_g = [60\%*(N_{cp1} + N_{cp2})+40\%*\Sigma\ (N_{spx})]/14 \qquad (1)$$

- N_g: represents the overall score, the overall score makes it possible to assess the level of maturity of the processes according to the scale which varies between 0 and 5.
- N_{cp1}: represents the maturity of the first core process for governance and IT risk management (EDM03).
- N_{cp2}: represents the maturity of the second core process for governance and IT risk management (APO12).
- N_{spx}: represents the maturity of the 12 supporting processes for governance and IT risk management (list mentioned above).

In the seventh step, we proceed to the description of the strengths / weaknesses identified of each process and we propose the action plans to be implemented to improve the level of maturity of the enabler "process".

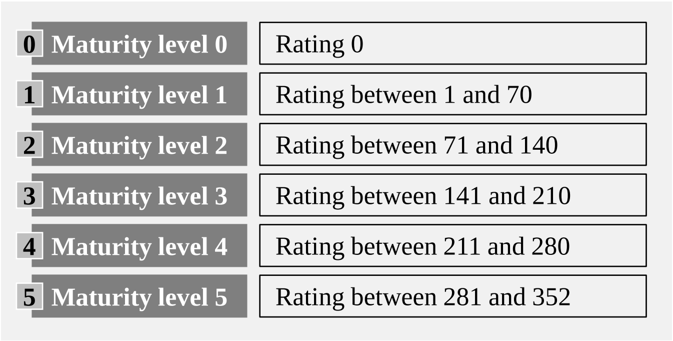
In the last step, we proceed to the preparation of the process maturity audit report in terms of IT risk management by resuming the various stages carried out and the audit results obtained.

In the remaining macro-phases going from 3 to 7, we only describe the two sub-steps "Definition of the analysis axes" and "Definition of a global maturity scale" of the planning step of the maturity audit. The rest remains similar to that of macro-phase 1.

C. *Maturity Audit of Organizational Structures related to IT Risk Management*

1) Definition of analysis axes: This step consists in determining the analysis axes based on the good practices of COBIT 5 [11]. The different axes of analysis and the corresponding rating system are described below (Table V).

2) Definition of a global maturity scale: In this step, we define a maturity scale that varies between 0 to 5 and is divided between the minimum score and the maximum score (Fig. 10).



0	Maturity level 0	Rating 0
1	Maturity level 1	Rating between 1 and 70
2	Maturity level 2	Rating between 71 and 140
3	Maturity level 3	Rating between 141 and 210
4	Maturity level 4	Rating between 211 and 280
5	Maturity level 5	Rating between 281 and 352

Fig. 10. Global Maturity Scale of the Enabler "Organizational Structures".

TABLE V. AXES OF ANALYSIS OF THE ENABLER "ORGANIZATIONAL STRUCTURES"

Analysis axe	Description	Rating system		
		0	1	2
Existence	Existence of the organizational structure to be audited	Non existent	Partially existent	Totally existent
Level of importance	Level of importance of the organizational structure to be audited: Core or supporting structure for IT risk management	Non existent	Supporting structure	Core structure
Operating principles	Description of the operating principles of the organizational structure to be audited	Non existent	Partially existent	Totally existent
Risk-based decisions	Taking into account the risks in the decision-making of the organizational structure audited	No	Partially	Yes
Span of control	Definition of the span of control of the organizational structure audited	No	Partially	Yes
Level of authority	Determination of the decisions that the organizational structure audited is authorized to take	No	Partially	Yes
Delegation of authority	Determination of the authorities that the organizational structure audited is authorized to delegate	No	Partially	Yes
Escalation procedures	Existence of a procedure for reporting incidents or problems encountered by the organizational structure audited	Non existent	Partially existent	Totally existent

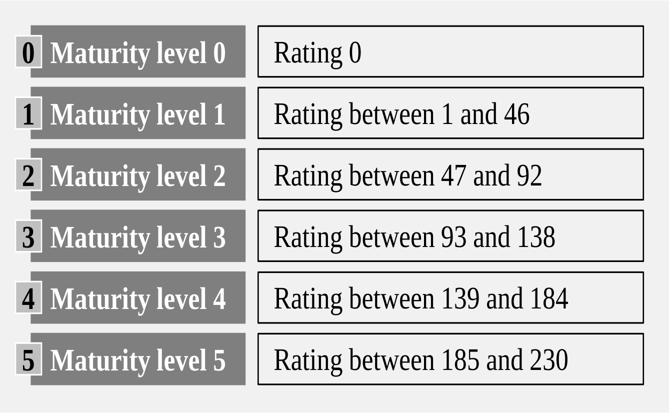
D. Maturity Audit of Culture, Ethics and Behaviour related to IT Risk Management

1) Definition of analysis axes: This step consists in determining the analysis axes based on the good practices of COBIT 5 [11]. The different axes of analysis and the corresponding rating system are described (Table VI).

2) Definition of a global maturity scale: In this step, we define a maturity scale that varies between 0 to 5 and is divided between the minimum score and the maximum score (Fig. 11).

TABLE VI. ANALYSIS AXES OF THE ENABLER “CULTURE, ETHICS AND BEHAVIOUR”

Analysis axe	Description	Rating system		
		0	1	2
Communication	Communication inside the organization on the desired behaviour	No	Partially	Yes
Awareness	Awareness inside the organization of the desired behaviour	No	Partially	Yes
Incentives / deterrents	The existence of bonuses / penalties in relation to the desired behaviour	Non existent	Partially existent	Totally existent
Re-evaluation of expectations	The existence of a re-evaluation of management's expectations in relation to the behaviour audited on the basis of a gap analysis between the existing behaviour and that desired	Non existent	Partially existent	Totally existent
Rules and norms	Clear definition of rules and norms regarding the desired behaviour	No	Partially	Yes



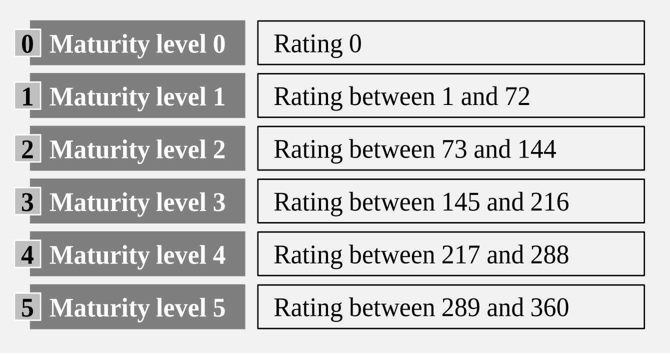
0	Maturity level 0	Rating 0
1	Maturity level 1	Rating between 1 and 46
2	Maturity level 2	Rating between 47 and 92
3	Maturity level 3	Rating between 93 and 138
4	Maturity level 4	Rating between 139 and 184
5	Maturity level 5	Rating between 185 and 230

Fig. 11. Global Maturity Scale of the Enabler “Culture, Ethics and Behaviour”.

E. Maturity Audit of the Information related to IT Risk Management

1) Definition of analysis axes: This step consists in determining the analysis axes based on the good practices of COBIT 5 [11]. The different axes of analysis and the corresponding rating system are described (Table VII).

2) Definition of a global maturity scale: In this step, we define a maturity scale that varies between 0 and 5 and is divided between the minimum score and the maximum score (Fig. 12):



0	Maturity level 0	Rating 0
1	Maturity level 1	Rating between 1 and 72
2	Maturity level 2	Rating between 73 and 144
3	Maturity level 3	Rating between 145 and 216
4	Maturity level 4	Rating between 217 and 288
5	Maturity level 5	Rating between 289 and 360

Fig. 12. Global Maturity Scale of the Enabler “Information”.

TABLE VII. ANALYSIS AXES OF THE ENABLER "INFORMATION"

Analysis axe	Description	Rating system		
		0	1	2
Existence	Existence of the audited information	Non existent	Partially existent	Totally existent
Information carrier / media	"The attribute that identifies the physical carrier of the information, e.g., paper, electric signals, sound waves." The audit focuses on the quality of this attribute.	Bad	Medium	Good
Information access channel	"The attribute that identifies the access channel of the information, e.g., user interfaces." The audit focuses on the quality of this attribute.	Bad	Medium	Good
Code / language	"Attribute that identifies the representational language/format used for encoding the information and the rules for combining the symbols of the language to form syntactic structures." The audit focuses on the quality of this attribute.	Bad	Medium	Good
Information type	"The attribute that identifies the kind of information, e.g., financial vs. non-financial information, internal vs. external origin of the information, forecasted/predicted vs. observed values, planned vs. realised values." The audit focuses on the quality of this attribute.	Bad	Medium	Good
Information currency	"The attribute that identifies the time horizon referred to by the information, i.e., information on the past, the present or the future." The audit focuses on the number of time horizons concerned.	A single time horizon	Two time horizons	Three time horizons
Information level	"The attribute that identifies the degree of detail of the information, e.g., sales per year, quarter, month." The audit focuses on the quality of this attribute.	Bad	Medium	Good
Retention period	"The attribute that identifies how long information can be retained before it is destroyed." The audit focuses on the quality of this attribute (in terms of time and manner of conservation)	Bad	Medium	Good
Information status	"The attribute that identifies whether the information is operational or historical." The audit focuses on the quality of this attribute.	Bad	Medium	Good
Novelty	"The attribute that identifies whether the information creates new knowledge or confirms existing knowledge, i.e., information vs. Confirmation." The audit focuses on the quality of this attribute.	Bad	Medium	Good
Contingency	"The attribute that identifies the information that is required to precede this information (for it to be considered as information)." The audit focuses on the quality and availability of the prerequisites of the information subject to the audit.	Bad	Medium	Good
Context	"The attribute that identifies the context in which the information makes sense, is used, has value, etc., e.g., cultural context." The audit focuses on the quality of this attribute.	Bad	Medium	Good

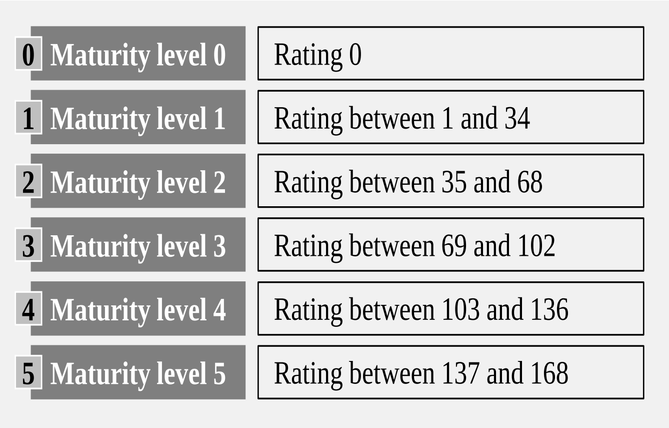
F. Maturity Audit of Services, Infrastructures and Applications related to IT Risk Management

1) Definition of analysis axes: This step consists in determining the analysis axes based on the good practices of COBIT 5 [11]. The different axes of analysis and the corresponding rating system are described below (Table VIII):

TABLE VIII. ANALYSIS AXES OF THE ENABLER “SERVICES, INFRASTRUCTURES AND APPLICATIONS”

Analysis axe	Description	Rating system		
		0	1	2
Existence	Existence of the service / infrastructure / application audited	Non existent	Partially existent	Totally existent
Functional	Service / infrastructure / application audited is functional	No	Partially	Yes
Architecture principles	Definition of architectural principles (for example: reuse, simplicity, agility)	No	Partially	Yes
Architecture viewpoints	Definition of architectural points of view (for example: model, catalogue, matrix)	No	Partially	Yes
Architecture repository	Existence of the architecture repository	No	Partially	Yes
Service level by service provider	Definition of service levels to be achieved by service providers	No	Partially	Yes

2) Definition of a global maturity scale: In this step, we define a maturity scale that varies between 0 and 5 and is divided between the minimum score and the maximum score (Fig. 13):



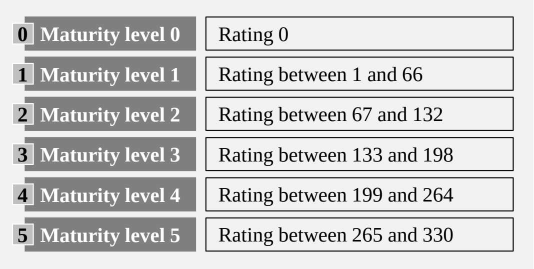
0 Maturity level 0	Rating 0
1 Maturity level 1	Rating between 1 and 34
2 Maturity level 2	Rating between 35 and 68
3 Maturity level 3	Rating between 69 and 102
4 Maturity level 4	Rating between 103 and 136
5 Maturity level 5	Rating between 137 and 168

Fig. 13. Global Maturity Scale of the Enabler “Services, Infrastructures and Applications”.

G. Maturity Audit of People, Skills and Competencies related to IT Risk Management

1) Definition of analysis axes: This step consists in determining the analysis axes based on the good practices of COBIT 5 [11]. The different axes of analysis and the corresponding rating system are described below (Table IX):

2) Definition of a global maturity scale: In this step, we define a maturity scale that varies between 0 and 5 and is divided between the minimum score and the maximum score (Fig. 14):



0 Maturity level 0	Rating 0
1 Maturity level 1	Rating between 1 and 66
2 Maturity level 2	Rating between 67 and 132
3 Maturity level 3	Rating between 133 and 198
4 Maturity level 4	Rating between 199 and 264
5 Maturity level 5	Rating between 265 and 330

Fig. 14. Global Maturity Scale of the Enabler “People, Skills and Competencies”.

TABLE IX. ANALYSIS AXES OF THE ENABLER "PEOPLE, SKILLS AND COMPETENCIES"

Analysis axes	Description	Rating system		
		0	1	2
Leadership skills	"Leadership skills include proactive leadership that sets clear direction that is aligned to the business outcomes and determination to ensure that the implemented policies deliver the effective disposition of risk."	Bad	Medium	Good
Analytical capability	"Capabilities to break down risk into risk factors that may prevent the achievement of goals and to assess those risk factors."	Bad	Medium	Good
Critical thinking	"Ability to make professional judgments about the value of additional information and determine whether a sufficient level of analysis has occurred is necessary."	Bad	Medium	Good
Interpersonal capabilities	"Ability to obtain information that is timely and accurate and to communicate with stakeholders who have different backgrounds and objectives."	Bad	Medium	Good
Communication	"Capability to communicate risk, risk factors, and the associated loss exposure in the context, language and priority of the relevant stakeholder."	Bad	Medium	Good
Influencing	"well-developed persuasion skills to help with adoption of risk practices across the enterprise and demonstrate value to stakeholders."	Bad	Medium	Good
Lateral thinking	"Risk needs to be approached differently depending on the type of risk."	Bad	Medium	Good
Technical understanding	"Basic understanding of the components comprising IT systems and how these components are connected to each other physically and logically."	Bad	Medium	Good
Organisational and business awareness	"To enable the enterprise to effectively plan, communicate and execute its risk management processes, the organisational points of contact, business units, goals, employee roles and responsibilities, and escalation paths must be documented and kept up to date."	Bad	Medium	Good
Risk expertise	"This skill refers to an understanding of the basic nature and composition of risk as well as ongoing improvement to keep pace with the dynamic nature of threats, vulnerabilities and impacts in the modern business environment."	Bad	Medium	Good
Training and coaching	"The ability to deliver targeted training programmes is essential in the successful update and sustainability of risk practices."	Bad	Medium	Good

V. CONCLUSION AND PERSPECTIVE

To respond to the limitations of existing standards dealing with IT Risk Management, we have defined in this article, a methodological approach to be adopted to conduct a maturity audit of IT risk management and we have presented a simplified IT risk management maturity audit system within an organization. The latter was built based on the best practices of "COBIT 5 for Risk" and by breaking down the seven enablers of COBIT 5 into seven macro-phases. The main purpose of the proposed system is to evaluate the maturity of IT risk management in an organization, identify the gaps and define the action plans to deploy in order to implement or update IT risk management within the organization. The simplified IT risk management maturity audit system proposed is declined into seven components to cover the different activities of an organization. The final delivery is a maturity audit report in terms of IT risk management covering the seven enablers defined by COBIT 5 (Fig. 2).

This work is a part of ongoing research for the development of a simplified IT risk management system. So, following the description of the IT risk management maturity audit system within an organization, we plan in a future work to design the system as well as to develop the IT solution that will support the execution of the audit steps.

REFERENCES

[1] AMF (Autorité des Marchés Financiers), Cadre de référence sur les dispositifs de gestion des risques et de contrôle interne, France: AMF Publication, 2010.

[2] S. P.Ferris, D. Javakhadze and T. Rajkovic, "CEO social capital, risk-taking and corporate policies," CEO social capital, risk-taking and corporate policies, pp. 46-71, 2017.

[3] J. S. Suroso and B. Rahadi, "Development of IT Risk Management Framework Using COBIT 4.1, Implementation In IT Governance For Support Business Strategy," in ICEMT, Singapore, 2017.

[4] A. Samimi, "Risk Management in Oil and Gas Refineries," Progress in Chemical and Biochemical Research, pp. 140-146, 2020.

[5] M. Gazeev and N. Volynskaya, "Contemporary limitations and development," Bulletin of Higher Educational Institutions, pp. 37-41, 2012.

[6] A. Samimi, S. Zarinabadi and M. Setoudeh, "Safety and Inspection for Preventing Fouling in Oil Exchangers," International Journal of Basic and Applied science, pp. 429-434, 2012.

[7] I. Osinovskaya and P. u. r. v. u. riska, "Management decision-making under risk," Economy and Entrepreneurship, pp. 767-770, 2015.

[8] COSO, Internal Control - Integrated Framework, COSO Publication, 2013.

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

[10] ISACA, "RELATING THE COSO INTERNAL CONTROL - INTEGRATED FRAMEWORK AND COBIT," ISACA Publication, USA, 2014.

[11] ISACA, COBIT 5 for Risk, USA: ISACA Publication, 2013.

[12] ISO, ISO/IEC 27000 : Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO Publication, 2018.

[13] ISO, ISO Guide 73 : Risk management — Vocabulary, ISO Publication, 2009.

[14] ISO, ISO 31000 - Management du risque, ISO Publication, 2018.

[15] ISO, ISO/IEC 27005:2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information, ISO Publication, 2018.

[16] A.-A. Walid and M. Basil, "A Code of Practice for Effective Information Security Risk Management Using COBIT 5," in 2nd International Conference Information Security Cyber Forensics, Cape Town, South Africa, 2015.

[17] H. M. Astuti, F. A. Muqtadiroh, E. W. T. Darmaningrat* and C. U. Putri, "Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk," in 4th Information Systems International Conference, Bali, Indonesia, 2017.

[18] ISACA, Risk IT Framework - 2nd Edition, USA: ISACA Publication, 2020.

[19] ISACA, Enabling Processes, USA: ISACA Publication, 2012.