IJCSI International Journal of Computer Science Issues, Volume 14, Issue 3, May 2017
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org https://doi.org/10.20943/01201703.4958

Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament

Malik MOTII[1], Alami SEMMA[2]

[1] Department of Mathematics and Computer Science, Faculty of Science and Techniques, Hassan 1st University,
Settat, Morocco

[2] Department of Mathematics and Computer Science, Faculty of science and Techniques, Hassan 1st University,
Settat, Morocco

Abstract

Despite the large number of options available, there has been considerable confusion over the different methods used by the IT manager due to their lack of compressive information.
this paper aims at studying the importance of IT governance (ITG) and proposing a new approach to pooling the references ITIL, COBIT with ISO / IEC 27002 for better use of the ITG in the Moroccan parliament. The latter is considered as a set of organizations with the task of legislative responsibilities, government control, evaluation of public policies, parliamentary diplomacy, and strengthening of parliamentary relations with constitutional institutions, Good governance, advanced regional workshops, civil society and citizens. Furthermore, this document will give the answer to a key question, whether the GSI should rely on the functions of the Moroccan parliament or should it envisage broader and more evolving objectives affecting the whole of government?
Keywords: Good practices, Moroccan Parliament, IT governance, ITIL, COBIT, ISO / IEC 27002.

1. Introduction

The ITG is a set of means that contribute to an efficient management and a synergy of all the components of its IT in order to derive the maximum profit. The ITG is a term frequently used in the world of information technology management, ITG focuses on strategic alignment, value creation, facilitates decision-making, Risk management, resource management and performance measurement to control information systems. ITG is an important element that is becoming increasingly important in the governance pyramid of any organization.
There are many references that reflect the best practices developed over the years. The reality is that each of them focuses on a specific issue: IT project management, quality, security, service management, IT audit, project development, performance, and so on.

COBIT (Control Objectives for Information and related Technology) Is a working tool for IT auditors. It replaced a book called JADIS "Control Objectives", which was a compilation of audit checklists to identify a number of good practices and checkpoints control. COBIT has taken its continuation by improving and enriching its content. From version to version, COBIT provided a set of rules for the effective management of IT governance.
ITIL (Information Technology Infrastructure Library) is a set of good practices structured as multiple processes communicating with each other. Each has its own role so that, at the end, they can both respond to the two issues which are: the continuous improvement and customer satisfaction.
ISO/IEC 27002 the ISO/IEC 27000-series standards are descended from a corporate security standard donated by Shell to a UK government initiative in the early 1990s. The Shell standard was developed into British Standard BS 7799 in the mid-1990s, and was adopted as ISO/IEC 17799 in 2000. The ISO/IEC standard was revised in 2005, and renumbered ISO/IEC 27002 in 2007 to align with the other ISO/IEC 27000-series standards. It was revised again in 2013.This article helps to highlight the completeness and pooling possible between these references based on the perspective of developing a version of COBIT 5 that includes the most used processes of ITIL and ISO 27001/27002.

2. COBIT

Definition
ISACA publishes a major version of its repository that strengthens integration and ITG in the governance of the organization.
COBIT becomes a unique and integrated repository, designed to help companies from the CEO to the CIOs through the business departments to achieve their objectives of governance and IT management. The main stake for organizations through

its stakeholders, it is the creation of value, it is defined by ensuring the balance between the realization of benefits, optimization of risks, and the efficient use of resources. The processes and good practices of COBIT are the result of a consensus of international experts, but also of many experiences. They aim to optimize IT investments, provide service delivery and propose metrics to be used to assess the capacity and level of performance of IT processes.
COBIT is constantly updated and harmonized with most other standards such as ITIL, CMMI, PMP, PRINCE2, TOGAF, etc. Since its first version released in 1996 COBIT has evolved, version 5 appeared in 2012.

COBIT 5, enablers are:

- Factors that, individually and collectively, influence whether something will work—in the case of COBIT, governance and management over enterprise IT
- Driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve
- Described by the COBIT 5 framework **in seven categories:**

1. **Processes** - Describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals
2. **Organizational structures** - Are the key decision-making entities in an organization
3. **Culture, ethics and behavior** - Of individuals and of the organization; very often underestimated as a success factor in governance and management activities
4. **Principles, policies and frameworks** - Are the vehicles to translate the desired behavior into practical guidance for day-to-day management
5. **Information** - Is pervasive throughout any organization, i.e., deals with all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
6. **Services, infrastructure and applications** -Include the infrastructure, technology and applications that provide the enterprise with information technology processing and services
7. **People, skills and competencies** - Are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions

COBIT 5 provides a framework for structured control IT operation with 37 processes divided into five areas:

- Evaluate, direct and monitor (EDM)
- Align, plan and organize (APO)
- Build, Acquire and implement (BAI)
- Deliver, service and support (DSS)
- Monitor, evaluate and assess (MES)

The five fields of COBIT include coherent sets of processes. EDM ensures compliance with major governance rules. The APO This area are the basics of IT management. The BAI is field to improve the processes of definition and implementation of computer applications. The DSS field its objective is to perfect the operation of the operation Computing. The MEA field details the basics of controlling information systems including internal control.

COBIT processes

For each of the 37 processes, COBIT describes the scope and purposes and then list and develop:

- Control objectives for IT auditors, which are detailed in other publications;
- A management guide written in a logic of governance SI;
- A maturity model for each process.

Evaluate, direct and monitor (EDM):

This area includes 5 processes. It ensures compliance with the main rules of governance:

- EDM1: Ensure Governance Framework Setting and maintenance
- EDM2: Ensure Benefits Delivery
- EDM3: Ensure Risk Optimization
- EDM4: Ensure Resource optimization
- EDM5: Ensure Stakeholder Transparency

Processes Align, plan and organize (APO):

This area includes 13 processes. These are the basics of IT management. The processes of this field are the following:

- APO1: Manage the IT Management Framework
- APO2: manage Strategy
- APO3: Manage Enterprise Architecture
- APO4: Manage Innovation
- APO5: Manage Portfolio
- APO6: Manage Budget and Costs
- APO7: Manage Human Resources
- APO8: Manage Relationship
- APO9: Manage service Agreements
- APO10: Manage Suppliers
- APO11: manage quality
- APO12: manage Risk
- APO13: Manage Security

Processes Build, acquire and implement (BAI):

This domain comprises 10 processes, the aim of this field is to improve the processes of definition and implementation of computer applications, the identification, development or acquisition of IT solutions, their implementation and integration with business processes, modification and maintenance of Existing systems. The processes of this area are the following:

- BAI1: Manage Programs and Projects
- BAI2: Manage Requirements Definition
- BAI3: Manage Solutions Identification and build
- BAI4: Manage availability and capacity
- BAI5: Manage Organizational Change Enablement
- BAI6: Manage changes
- BAI7: Manage change Acceptance and transitioning
- BAI8: Manage Knowledge
- BAI9: Manage assess

- BAI10: manage configuration

Processes Deliver, Service and Support (DSS)

This domain includes 6 processes. This area covers the implementation of services: computer operations, security management, continuity management service, user support, data management and equipment. The processes of this area are the following:

- DSS1: Define and manage operations
- DSS2: Manage service Requests and incidents
- DSS3: Manage problems
- DSS4: Manage Continuity
- DSS5: Manage security services
- DSS6: Manage business process Controls

Processes Monitor, Evaluate and Assess (MEA):

This area includes 3 processes. It details the foundations of the control of information systems including internal control, performance management, compliance with regulatory standards and governance. The processes of this field are the following:

- MEA1: Monitor, evaluate and assess the performance and conformance
- MEA2: Monitor; evaluate and assess the system of internal control
- MEA3: Monitor, Evaluate and assess compliance with external requirements

Elements of governance:

However, COBIT 5 is struggling to come up with a complete IS governance approach as it approaches by computing. Now, it will never be said enough IT is not SI. They are two different universes even if they have something in common. Result: COBIT 5 sees only part of SI governance, that in relation to IT. The concept of IS governance is broader.

Before going any further, let's analyze what COBIT 5 says about governance. First, there are two very important processes that determine the logic of governance:

- EDM 01: " Ensure Governance Framework Setting and maintenance"
- EDM 05: " Ensure Stakeholder Transparency"

There are then five processes concerning the positioning of the IT approach within the framework of the organization:

- APO 01: "Manage the IT management framework. "
- APO 02: "Managing strategy"
- APO 03: "Manage Enterprise Architecture"
- APO 04: "Manage innovation"
- APO 05: "Manage portfolio"

It is very interesting but it is an approach to IT and not an approach oriented to the IS.

Then COBIT 5 is interested in the changes. It is indeed a delicate moment: after the project, we must get to start the application and make it work. It is based on three important processes:

- BAI 05: "Manage Organizational Change Enablement"
- BAI 06: “Manage Changes”
- BAI 07: "Manage change Acceptance and Transitioning"

Finally, we must not forget the internal control with the process:

- MEA 02: " Monitor; evaluate and assess the system of internal control".

As can be seen, COBIT 5 marks a significant evolution of the repository towards IS governance with a total of 11 processes out of 37. This is not bad. Despite this, the document remains globally very oriented towards the computer technologies. It ignores the main areas of information systems governance, in particular:

- The design of information systems:
  An information system, whatever it may be, is built on an overall design. The quality of this approach largely determines the effectiveness of the information system.
- The functioning of information systems:
  It is important to ensure that the information system operates on a regular and efficient basis. It must be ensured that it is efficient and secure. A manager must manage and manage each information system.
- The management of information systems:
  Modifications to the information system are made over a period of time. It is therefore necessary to control these operations. The loss of control of this process results in a significant deterioration of the information system.
- The evolution of information systems
  Changes to the information system require strategic thinking, a planned approach and control of the operations carried out.

These four areas are at the heart of the governance of information systems. As can be seen, COBIT covers only part of IF Governance.

3. ITIL

ITIL, formerly an acronym for Information Technology Infrastructure Library, is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. (ITIL).

Responding to growing dependence on IT, the UK Government’s Central Computer and Telecommunications Agency (CCTA) in the 1980s developed a set of recommendations. It recognized that, without standard practices, government agencies and private sector contracts had started independently creating their own IT management practices.

In ITIL 2011 edition ITIL publish 5 main volumes that define ITSM (IT service management) stage which are:

- ITIL Service Strategy: understands organizational objectives and customer needs.
- ITIL Service Design: turns the service strategy into a plan for delivering the business objectives.
- ITIL Service Transition: develops and improves capabilities for introducing new services into supported environments.
- ITIL Service Operation: manages services in supported environments.
- ITIL Continual Service Improvement: achieves services incremental and large-scale improvements.

Key benefits of ITIL:

Manage business risk and service disruption or failure

Improve and develop positive relationships with your customers by delivering efficient services that meet their needs

Establish cost-effective systems for managing demand for your services

- Support business change whilst maintaining a stable service environment.

To define ITIL, you must be in a context of continuous improvement and customer orientation needs.

ITIL is a set of good practices structured as multiple processes communicating with each other. Each has its own role so that, at the end, both can respond to the two issues which are: the continuous improvement and customer satisfaction.

The good practices provide organizations a structure, approved by years of experience in large companies globally recognized for their professionalism and thoroughness, to formalize their processes and manage their information. These good practices are used primarily as guidelines to companies serving businesses wishing to improve their quality of service.

Objectives of ITIL

ITIL provides a pragmatic approach to deal with the situations in which CIOs are faced, namely, among others:

- The IT sector is receiving more and more investment budget. It represents important expenses especially for companies to whom; the main business isn't focused on computing.
- Information systems are becoming more complex. As long as the IT workers are trying to meet the requirements and demands of their internal customers, they find themselves facing an infrastructure and a large arsenal application that must be managed and maintained while trying to be responsive.
- With the advent of new technologies of information and communication (social medias …), users have become up - to - date with all high - tech news. Especially since the editors have popularized their software's (advent of open source) and telecommunications infrastructure (mobile phone).
- As long as companies have spent enormous sums of money for the IT infrastructure (hardware and software), the leaders expect a return on investment and begin to tighten the budgets. Thus, the difficult situations the CIOs have to face.
- Globalization has played its part too. It introduced the practices of service between recharges its subsidiaries. This new situation has opened the eyes of CIOs who want to bill their services to their internal customers.
- All this was said, made the ambiguous role of the CIO. With the mode of outsourcing, the user begins to ask questions about the added value of CIOs as external suppliers support their claims with contracts and a better reactivity.
- For companies specialized in IT, being certified or certifying their staff improve their reputation and trust of their internal or external customers. This certification is a label that the CIO can show to proof their professionalism with standards recognized worldwide.

Client axis:

For this axis, ITIL will respond to the:

- Lack of mechanism structured for delivery and service support.
- Lack of confidence in the management of IT services.

Management axis:

- Mismanagement of resources and means.
- Failure of service in a frequent way.
- Irregularity in meeting the deadlines of requests and claims of customers.
- Changes or modifications not coordinated or analyzed.

Decision axis:

- Decisions are made without any pragmatic basis.

The basic concepts of ITIL

Mainly, ITIL is based on five pillars:

- Customer focus.
- The life cycle of service.
- The concept of process.
- Continuous improvement.
- Communication.

Customer focus

This concept is crucial for managing IT services. It makes the customer needs the main concern of the IT specialist. Thus, what's important is not focusing on new technologies and the power of servers and telecommunications but rather meeting the functional need of the customer in the most faithful and most optimal way.

Taking into consideration the business needs of the customer and make them the main concern of the IT management is the reason to be of the IT services.

It is then necessary to fully understand the customer needs, follow up their development and establish an organization that supports them expressing and monitoring these needs.

The life cycle of service

Before describing the life cycle of the service, we must first explain its concept. In general, the service can be defined depending on the context.

In a restaurant, we can evaluate the service: smiles, atmosphere, responsiveness, ...

In a tennis match, the service is a trigger of play in an organization, a service is an entity having a function and a task performed by a group of staff. In the IT field, a service is defined as a benefit, help or assistance a user can expect from a supplier.

In daily life of IT projects, and after the post - production of projects, CIOs find themselves faced with two situations:

- Whether the operations team was not involved in the project since its design, creating a frustration having to deal with tasks from which they don't understand the point in the business.
- Or the project team, as it masters the issue, continue the project in the operational phase. This generates organizational failures and conflicts of responsibility.

To avoid this kind of anomaly, ITIL provides the solution and advocates considering the management of services from the needs study of the IT projects. Thus, the overlapping roles of the project team and operations team are avoided and the operating team is aware of the stakes of the project and its services as well as the added values.

This makes sure that the resources and expertise required for the operation of services after their releases are available. This involves taking into consideration the impact of performance, availability and budget since the start of the project.

The process concept

The concept of life cycle brings all necessary elements for successful projects from the specification of needs by customers until the go - live of services.

The concept of process has demonstrated its robustness when quality is the matter. ITIL has adopted this approach to structure the philosophy of its good practices as multiple processes interacting between each other. This concept of process provides answers to the sequence of activities while undergoing examinations and performance indicators measuring the achievement of results for which the process was designed.

The process owner is responsible for the design of the process and ensures that it meets the need defined. He reports to company executives.

The process manager is responsible for implementation of the process as it was defined by process owner to which he reports.

The quality of service

This concept is the raison d'être of the good practices. Quality service is defined as it has the ability to respond to customer needs exactly as they were defined. The client judges their supplier, not based on their how - to methods but rather based on their appreciation of the result within the deadline expected, while respecting the specifications defined.

In that sense, ITIL seeks to improve service in a perpetual manner based on the philosophy of Deming wheel: Plan, Do, Act, Check.

4. ISO/IEC 27002

In particular, the relationship between ISO / IEC 27001 and ISO / IEC 27002 does not always seem clear to researchers. (Note: ISO / IEC 27001 is the standard containing formal requirements, ISO / IEC 27002 is the code of practice which gives guidance on the implementation of the standard).

ISO / IEC 27002 is an international standard on information security, jointly published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), revised in 2013, whose title in French is - Security techniques - Code of practice for information security management. It is part of the ISO / IEC 27000 suite.

ISO / IEC 27002 is a set of 114 "best practices" measures intended to be used by all those responsible for setting up or maintaining a Safety Management System. Information (WSIS). Information security is defined within the standard as "preserving the confidentiality, integrity and availability of information".

This standard is not mandatory for companies. However, compliance may be mentioned in a contract, so a service provider may commit to respecting standardized practices in its dealings with a customer.

ISO / IEC 27002 is more a code of practice, a true standard or a formal specification such as ISO / IEC 27001. It contains a series of controls (35 control objectives) which suggest taking into account risks Confidentiality, integrity, and availability information. Companies that adopt ISO / IEC 27002 should evaluate their own information security risks and apply appropriate controls, using the standard to guide the company. ISO 27002 is not a standard in the usual sense. It is not a technical, technological or product-oriented standard or a methodology for evaluating equipment such as the common CC / ISO 15408 criteria. It is not a Does not lead to certification, as this domain is covered by ISO / IEC 27001 in its relations with a customer.

The guiding principles:

ISO/IEC 27002:2013 are the initial points for implementing information security. They rely on either legal requirements or generally accepted best practices.

Measures based on legal requirements include:
- Protection and non-disclosure of personal data
- Protection of internal information
- Protection of intellectual property rights

Best practices mentioned in the standard include:
- Information security policy
- Assignment of responsibility for information security
- Problem escalation
- Business continuity management

When implementing a system for information security management, several critical success factors should be considered:
- The security policy, its objectives and activities should reflect the business objectives.
- The implementation should consider cultural aspects of the organization.
- Open support from and engagement of senior management should be required.
- Thorough knowledge of security requirements, risk assessment and risk management should be required.
- Effective marketing of security should target all personnel, including members of management.

The security policy and security measures should be communicated to contracted third parties.
- Users should be trained in an adequate manner.
- A comprehensive and balanced system for performance measurement, which supports continuous improvement by giving feedback, should be available.

Content of the standard:

ISO / IEC 27002 consists of 18 chapters, the first four of which introduce the standard and the following 14 chapters cover safety management in both its strategic and operational aspects.

The standard starts with 5 introductory chapters:
0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Structure of this standard

These are followed by 14 main chapters:

5. Information Security Policies
6. Organization of Information Security
7. Human Resource Security
8. Asset Management
9. Access Control
10. Cryptography
11. Physical and environmental security
12. Operation Security- procedures and responsibilities, Protection from malware, Backup, Logging and monitoring,

Control of operational software, Technical vulnerability management and Information systems audit coordination
13. Communication security - Network security management and Information transfer
14. System acquisition, development and maintenance - Security requirements of information systems, Security in development and support processes and Test data
15. Supplier relationships - Information security in supplier relationships and Supplier service delivery management
16. Information security incident management - Management of information security incidents and improvements
17. Information security aspects of business continuity management - Information security continuity and Redundancies
18. Compliance - Compliance with legal and contractual requirements and Information security reviews

5. (Comparison between COBIT, ITIL and ISO 27002)

Table 1. Comparison between COBIT, ITIL and ISO 27002

AREA	COBIT 5	ITIL V3 2011	ISO/IEC 27002 2013
Function	Mapping IT process	Mapping Service Level Management	Information Security framework
Area	5 areas and 37 processes	28 processes	14 chapters 114 measures
Issue	ISACA	OGC	ISO Board
Implementation	Accounting Firm, IT consulting Firm	Manage Service Level	Compliance to security standard

GENERAL PURPOSE:

- COBIT is a high-level framework (relative to ITIL, ISO 27002 and NIST) that maps core IT processes in a manner that allows governance bodies – usually business executives – to successfully execute key policies and procedures. Similar to ISO 27002, it answers the 'what' that is being managed, as opposed to the 'how' answered by ITIL. However, whereas ITIL and ISO 27002 are focused only on information security, COBIT allows for a much broader scope, taking into account all of IT management processes.
- ITIL is a set of best practices an organization may implement in order to align IT resources and offerings to business goals. It is offered in a series of five core publications each corresponding to a stage in the lifecycle of IT. This process produces documentation of processes, tasks and checklists not specific to the organization with a goal of being able to create a baseline from which to implement controls and measure success.
- ISO27001 produced by the ISO (International Organization for Standard). Formulates a management system that to control information security, it does not provide specific controls.

Interactions:

- ITIL was designed as a service management framework to help understand how support processes, how deliver services.
- COBIT was designed as an IT governance model, particularly and initially with audit in mind to give control objectives and control practices on how that process should behave.
- The difference between the two is, COBIT tells what should be doing, while ITIL tells how should be doing it Put COBIT and ITIL together, and have a very powerful model of what need to be doing and how need to be doing it, when it comes to process management.
- Basically, ISO gives security, but does not provide to acknowledge of how to integrate them into business process.
- ITIL focus IT processes.
- COBIT focuses on control and metrics.
- So, a combination of all three is usually the best approach. COBIT can be used to determine if the company's needs are being properly supported by IT.
- ISO can be used to determine and improve upon company's security posture. And ITIL can be used to improve IT processes to meet the company's goals (including security).

6. Towards a pooling of COBIT, ITIL and ISO/IEC 27002.

ITIL structures its approach of the services' management around the relationship with stakeholders: daily IT service users and project managers for controlling. COBIT, in the same way, has systematically put beforehand the finality of IT services, including meeting the needs and the desire to align supply with demand. Both approaches share the same values regarding the management of IT services.

ISO/IEC 27002, COBIT AND ITIL SO DIFFERENT BUT IS THERE AN OPPORTUNITY TO POOL, the goal of ISO/IEC 27002:2013 is to provide information to parties responsible for implementing information security within an organization. It can be seen as a best practice for developing and maintaining security standards and management practices within an organization to improve reliability on information security in interorganizational relationships.
The figures below list the COBIT processes and ISO/IEC 27002 measures that are closest to the ITIL processes. Note that the names of the process are often the same, reflecting the growing awareness of ITIL with COBIT designers.

Table 2. Combination COBIT and ITIL

Number process COBIT 5 / 37		**ITIL 2011 / Phase 28 process**					**Total Combination with ITIL**
		SS	***SD***	***ST***	***SO***	***CSI***	
EDM	3	3	0	0	0	0	3
APO	9	7	7	0	0	3	17
BAI	8	0	5	8	0	0	13
DSS	5	0	2	0	5	0	7
MEA	3	0	0	0	0	3	3
Total	28	10	14	8	5	6	43
No Combination with ITIL: 9					**No Combination with COBIT 5: One Process in SO Phase**		
EDM1	APO3	BAI3	DSS6	Problem Management			
	APO4						
EDM3	APO7	BAI5					
	APO13						

Table 3. Combination ISO/IEC 27002 with ITIL

Sections of ISO/IEC 27002 and measures		measures Coverts	ITIL				
			SS	SD	ST	SO	CSI
A5	2	2	-	2	-	-	-
A6	7	7	-	4	-	3	-
A7	6	3	-	-	-	3	-
A8	10	9	-	2	7	-	-
A9	14	12	-	-	1	11	-
A10	2	0	-	-	-	-	-
A11	15	8	-	2	-	6	-
A12	14	12	-	3	3	6	-
A13	7	3	-	-	-	3	-
A14	13	3	-	3	-	-	-
A15	5	5	-	5	-	-	-
A16	7	7	-	-	-	7	-
A17	4	4	-	-	-	4	-
A18	8	5	-	1	-	4	-
Coverts	**114**	80	0	22	11	47	0
No Coverts		**34**					

7. Why pooling?

The objective is to cover all the main activities of the Moroccan Parliament and in particular IT, seeks to identify principles of governance and to identify the process and best practices to be applied, to deal with end-to-end management of Information and related technologies with better security of exchanges and information management. The COBIT, ITIL and ISO/IEC 27002 steps are often performed separately. ITIL to better structure service centers, which for the same reason are the only function to be represented as a better tool for managing process-based services (the core of the process). The service center procedures for managing incidents (structuring levels, escalation, ticketing, resolution of enrichment databases, etc.) have been developed to meet lower cost demands.

Most of the support functions are outsourced, which were not necessarily in the core business and seem complicated to manage and optimize internally due to poor control, poor management, lack of competencies and low rate of ICT staff. In terms of tools, publishers have provided the best performers, capable of managing all procedures and linking them to a broadly-based resource database (calling tickets, configuration objects, but also job descriptions, Etc.). All this "arsenal" was built with the ITIL framework.
The key points to consider in the order of sharing the two approaches are as follows.

• Reconcile two cultures
ITIL culture is pragmatic, constantly confronted with the daily issues and geared more towards the service (service continuity, performance). it often manages data objects in a level of detail that only applies to players in the support, maintenance or operation.

COBIT, however, may be perceived as too theoretical, not often useful nor concrete enough to be deployed easily and effectively.

• Structuring the whole repository
Avoid duplication of processes, which inevitably occurs if one does not describe a mapping process to ensure overall consistency.

- **Make the link with the studies and developments**

ITIL has trouble spread to the teams of studies and development. It is recognized neither in the management of projects at the elementary level or in the overall management of portfolios and investments.

- **Gradually build the data of the ISD model**

ITIL gains are interesting but the risk of falling into the details is big. We must rely on the CMDB to create the data model of the CIO, ensuring distance themselves and define the granularity of the data relevant for control.

8. Total Combination between COBIT, ITIL with ISO/IEC 27002

This chapter shows the inverse relationship and approximation between the phases and processes of the two COBIT 5 and ITIL v3 references and the ISO / IEC 27002 control objectives
This chapter is not intended to be final or prescriptive. Relationships are displayed only at the high level, indicating just the combinations between them.

COBIT AND ITIL

Reconciliation of phases

- Evaluate, direct and monitor (EDM) => ITIL 'SS'
- Align, plan and organize (APO) => ITIL 'SS','SD','CSI'
- Build, Acquire and implement (BAI) => ITIL 'SD','ST'
- Deliver, service and support (DSS) => ITIL'SD','SO'
- Monitor, evaluate and assess (MEA) => ITIL 'CSI'
-

Reconciliation of processes

- EDM1: Ensure Governance Framework Setting and maintenance == SS - Service portfolio management
- EDM2: Ensure Benefits Delivery
- EDM3: Ensure Risk Optimization
- EDM4: Ensure Resource optimization == SS - Financial management for IT services
  EDM5: Ensure Stakeholder Transparency == SS - Business relationship management

- APO1: Manage the IT Management Framework == SD - the seven-step Improvement process
- APO2: manage Strategy == SS - Strategy management for IT Services
- APO3: Manage Enterprise Architecture
- APO4: Manage Innovation
- APO5: Manage Portfolio == SS - Service portfolio management, SD - Service catalogue management

- APO6: Manage Budget and Costs == SS - Financial management for IT services, SD - Capacity management
- APO7: Manage Human Resources
- APO8: Manage Relationship == SS - Financial management for IT services, SS - Business relationship management, CSI - Service reporting
- APO9: Manage service Agreements == SS - Service portfolio management, SS - Financial management for IT services, SD - Service catalogue management, SD - Service-level management, SD - Supplier management
- APO10: Manage Suppliers == CSI - the seven-step Improvement process
- APO11: manage quality == SD - Security management
- APO12: manage Risk == SD - Security management
- APO13: Manage Security
- BAI1: Manage Programs and Projects == SD - Design coordination
- BAI2: Manage Requirements Definition == SD - Service-level management
- BAI3: Manage Solutions Identification and build
- BAI4: Manage availability and capacity == SD - Availability management, SD - IT service continuity management
- BAI5: Manage Organizational Change Enablement
- BAI6: Manage changes == ST - Change management
- BAI7: Manage change Acceptance and transitioning == SD - Design coordination, ST - Transition planning and support, ST - Release and deployment management, ST - Service validation and testing, ST - Change evaluation
- BAI8: Manage Knowledge == ST - Knowledge management
- BAI9: Manage assess == ST - Service asset and configuration management
- BAI10: manage configuration == ST - Service asset and configuration management
- DSS1: Define and manage operations== SO - Event Management
- DSS2: Manage service Requests and incidents == SO - incident Management, SO - Access Management
- DSS3: Manage problems == SO - Request Fulfillment
- DSS4: Manage Continuity == SD - IT service continuity management
- DSS5: Manage security services == SD - Security management DSS6: Manage business process Controls == SO - Incident Management
- MEA1: Monitor, evaluate and assess the performance and conformance == CSI - Service reporting
- MEA2: Monitor; evaluate and assess the system of internal control == CSI - the seven-step Improvement process
- MEA3: Monitor, Evaluate and assess compliance with external requirements == CSI - the seven-step Improvement process

ITIL WITH ISO/IEC 27002

• The objective of ITIL is to organize infrastructure and IT assets in contrast to ISO / IEC 27002 to organize and secure the Information Systems Security Management System (ISMS) in a broad sense, ITIL consists of 5 sentences 28 processes and 4 functions) ISO / IEC 27002 of 14 sections and 114 safety measures.

• ISO / IEC 27002 uses PDCA methods in projects as an approach, ITIL is modular (Process) in PDCA.

The sections most covered by ITIL are:
AT 5. Information security policies
A6. Organization of information security
AT 8. Asset Management
AT 12. Operation Security-procedures and responsibilities, Protection from malware, Backup, Logging and monitoring,
A15. Supplier relations - Supplier relations
A16. Communications security
And A17. Information security aspects of business continuity - Information security continuity and Redundancies
This explains their reconciliations such as the ISM (Information Security Management) or standards-based, such as continuity plans.
Other sectors are partially covered by ITIL processes with coverages such as physical and environmental security, access management, and operations and telecommunications management because they are not compatible with ITIL methods, (11.1.4, 11.2.3, 13.2.1)
• Lightly covered sections A7, A11, A13, A14, A18;
• Not Covered A10;
• No HR connection;
• A12 and A17 are present within the scope of good practice but not with the rigidity imposed by the ISO / IEC 27002 measurements.

ITIL processes not covered by ISO / IEC 27002:
[1] Generation of strategy, [2] Demand management, [3] Financial management, [4] Service portfolio management, [5] Service catalog management.
The uncovered phases of ITIL are:
SS: Service Strategy.
CSI: Continual Service Improvement.
So, there is a limitation by the ITIL Framework because it actually complements the ITIL IT perimeter and to have a good WSIS in the broad sense including HR, Security of exchanges between systems or cryptography of information, rate 30 % Present measures not covered by ITIL and 70%, measures covered by ITIL.

9. Bequest for a successful approach for pooling

There is no doubt that effective management policies and procedures ensure that information technology is managed as a common part of everyday activities. The adoption of standards and best practices allows rapid implementation of good procedures and avoids long delays in the creation of new approaches when reinventing wheels and adopting appropriate methods.
COBIT and ITIL offer a top-down approach for IT governance and service management when used together, The COBIT management guide provides a comprehensive approach to managing objectives and priorities for IT activities. COBIT separates itself between governance and IT management.
When used together, the power of both approaches is amplified, with a greater likelihood of support and direction, and more efficient use of resources for implementation.

While being widely scoped is can be viewed as a strength for COBIT, it can also be a detractor during implementation. Being by design not limited to a single area, it can often lead to gaps in coverage.
While focused on information security only, ITIL is considered to be a higher-level standard than ISO / IEC 27002, and points to ISO standards for detailed implementation. Specific implementation details are rather lacking.
ISO / IEC 27002 is focused specifically and purposefully on information security and is therefore limited in scope compared to other standards such as COBIT.
Similar to ISO / IEC 27002, NIST is limited in scope to information security, whereas COBIT and ITIL are more general in nature.

Structuring the process

The organization needs an effective action plan that suits their particular circumstances and the needs, but some recommendations are common to all businesses:

- Ensure that the project of setting up standards of governance is in terms of senior management and will be sponsor of this project.
- Deficiencies and ensure that IT issues are identified and listed
- Work with management in ensuring alignment of initiatives with positive impacts on business activities of the company.
- Developing dashboards to measure the performance of IT services

Planning

Establish an organizational framework (ideally as part of a global initiative of IT governance) with clear responsibilities and objectives.
Ensure the participation of all stakeholders.

- Align IT strategy with business goals
- Understand and define the risks
- Define target areas and identify the process areas in IT that are critical to delivering value and managing these risk areas
- Develop strategies for improvement, and decide of the highest priority projects that will improve management and governance.
- Consider supporting COBIT control objectives using the most detailed ITIL guidelines.
- Measure results, establish a dashboard mechanism to measure current performance and monitor the results of further improvements.

Pitfalls to avoid

There are also some obvious rules, but pragmatic, that management should follow to avoid the pitfalls:

- Treat the initiative to implement a project activity with a series of phase.
- The implementation involves cultural change and new processes. Therefore, a key success factor is the activation and motivation for change.
- Make sure there is a clear understanding of objectives.
- Manage wait times. In most companies, achieving success takes time and requires continuous improvement.
- Focus first on where it is easier to make changes and improvements and build from there, one step at a time.

10. Conclusions

Over the years, there are a number of methodologies and standards designed to assist IT governance and information security within modern organizations in order to achieve an optimal process to achieve their goals.
Major organizations continue to use various mechanisms to ensure that their IT infrastructure is aligned with their business objectives and core business and complies with local and global IT governance rules and regulations.
Good IT governance does not exist in a vacuum. Unless IT governance practices are institutionalized as part of a formal process that is regularly assessed and updated in light of changes in parliament or technology, nothing will work. Irrespective of the methodology, ITG's objective is to improve the organization's competitive advantage, optimize operations and mitigate risks.
The truth is that IT governance is an integral part of a modern organization that must be meager, nasty and must measurably complement the core business objective.
In this discussion, the proposed suggestion is the design of a version that integrates most of the subsequent development processes within the ITG framework, and based on the principles of IT service life cycles, their securing such as cycle Of service life proposed by the ITIL methodology which should also be used to define strategies, concepts and processes; COBIT should be used to assess critical success factors and ISO / IEC 27002 should guide IT in relation to IT management and security issues, depending on the parliamentary work that requires document security. Committees and parliamentary groups. With a good ITG one can also have very good governance over all the functions of the Moroccan parliament and this can increase the broader and evolving objectives that affect work, control and the entire government.

References

[1] Information technology — Security techniques — Code of practice for information security management https://www.ansi.tn/fr/documents/comparatif_ISO27002_2013-2005.pdf
[2] Abdelaali Himi & Samir Bahsani and Alami SEMMA The-IT-Service-Managementaccording-to-the-ITIL-framework-applied-to-the-enterprisevalue-chain, http://ijcsi.org/papers/IJCSI-8-3-2-515-522.pdf
[3] Samir BAHSANI, Abdelaali HIMI, Hassan MOUBTAKIR and Alami SEMMA Towards-a-pooling-of-ITIL-V3-and-COBIT, http://ijcsi.org/papers/IJCSI-8-6-2-185-191.pdf
[4] ITIL pour un service informatique optimal- Christan du mont - Edition Eyrolles
[5] Pour une meilleure gouvernance des systèmes d'information - Dominique Moisand; Fabrice Garnier de Labareyre Edition Eyrolles 2009
[6] Mapping of ITIL v3 with COBIT® 4.1 IT Governance Institute www.itgi.org
[7] C. Dumont. − ITIL pour un service informatique optimal (2e édition).
[8] C. Dumont. − Mémento ITIL.

[9] E. Besluau. − Management de la continuité d'activité.
[10] Gouvernance des Systèmes d'Information http://gouvsi.blogspot.com/2014/10/cobit-5-en-francais-un-progres.html
[11] A Comparison of COBIT, ITIL, ISO 27002 and NIST. (2016, 03 04). agnosticationater.blogspot.com.tr: http://agnosticationater.blogspot.com.tr/2013/12/a-comparison-of-cobit-itil-iso-27002.html
[12] A comparison of the business and technical drivers for ISO 27001, ISO 27002, COBIT and ITIL. (2016, 03 04). http://trongbang86.blogspot.com.tr/: http://trongbang86.blogspot.com.tr/2010/11/comparison-of-business-and-technical.html
[13] Arora, V. (2016, 03 03). Comparing different information security standards: COBIT v s. ISO 27001. Qatar CMU: https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf
[14] (2016, 03 03). Key Benefits Of ITIL. Axelos: https://www.axelos.com/best-practice-solutions/itil/key-benefits-of-itil
[15] Verma, M. (2016, 04 03). Comparison of it governance framework-COBIT, ITIL, BS7799. Slideshare.net: http://www.slideshare.net/meghnaverma3956/comparison-of-it-governance-frameworkcobit-itil-ds
[16] Aligning COBIT ITIL V3 ISO27002 for Business Benefit a Management Briefing from ITGI and OGC Http://www.isaca.org/Knowledge Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf
[17] A Comparison of COBIT, ITIL, ISO 27002 and NIST *http://agnosticationater.blogspot.com/2013/12/a-comparison-of-cobit-itil-iso-27002.html*

MALIK MOTII is a Ph.D. student 'The IT governance for the Moroccan Parliament', Department of Mathematics and Computer Science, Faculty of Science and Technology, Hassan 1st University, Settat, Morocco. Currently an engineer specialized in networks and information systems, information technology manager networks of information systems in the house of Counselors, Moroccan parliament.

ALAMI SEMMA is a Ph.D. in Faculty of Science and Technology, Hassan 1st University, Settat, Morocco. He is a qualified professor in electrical engineering.