International Journal of Mathematics and
Computer Science, **16**(2021), no. 1, 47–66

A Conceptual Hybrid Approach for Information Security Governance

Mounia Zaydi, Bouchaib Nassereddine

Faculty of Science and Technology
577 SETTAT, Morocco

email: m.zaydi@uhp.ac.ma, bouchaib.nassereddine@uhp.ac.ma

(Received May 5, 2020, Accepted June 2, 2020)

Abstract

Despite the technological advancements in information system security (ISS) and the availability of relevant IT frameworks, standards, and mechanisms of control and security, statistical trends in data breach reveals a growing threat to organization's security system. This is mainly due to the independent and separate use of these approaches. To address this, a vision of governance based on an integrated and holistic ISS perspective required. The research findings lead to design a new integrated model of ISS-GOV, including three essential dimensions: IT governance (IT-GOV), IT security management (ITSecM) and IT service management (ITSM). To this end, we are going to use approaches proven successful for these 3 disciplines around the world, most notably ITIL, COBIT and ISO27001, as well as ensuring continuous improvement through the quality approach of PDCA.

1 Introduction

Increasingly, organizations are more and more aware of the importance of an effective information security program. As a result, they are starting to implement the basic and essential components to ensure the security of their information assets (firewalls, Security policies, IDS, Anti-X, etc.) [1]. Commonly, these pieces are generally the responsibility of a small team of

Key words and phrases: Information security; IT-GOV, ISS-GOV, ITSM, ITSecM.
AMS (MOS) Subject Classifications: 68U35.
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

security staff who are responsible for ensuring the entire company can resist any form of internal or external threat-, which is nearly impossible. Given the fact that any business can no longer separate from the IT, maintaining a competitive advantage [2] means that CIOs will have to anticipate risks that can have a significant impact on the organizations strategic assets, which means that they must invest in the company's resources to manage the security system for their information. The ISS-GOV is a subset of C-GOV related to the Information security topics [3]. Information security is often considered a purely technical issue. However, the progress of any organization relays on the security of their information assets, executives must ensure that ISS processes are part of the core business operations. The most effective way to achieve this objective is to focus on the ISS-GOV as part of internal controls and policies that take part of corporate governance. Up to recently, it was difficult for organizations to have a coherent framework for guiding their ISS-GOV endeavors. In this perspective, a wide range of standards and approaches have emerged, but none of them can meet all the requirements of the ISS-GOV. None of them cover all aspects of the ISS-GOV; authors have to use different frameworks, which implies an additional cost. The desired framework must cover IT service, security management and IT governance. The basic objectives of the ISS-GOV are to provide: IT-GOV, ISS risk management, ISS management, resource management, incident and change management [4]. To achieve these objectives, the use of COBIT is a very appropriate option; even though it is often perceived as complicated and organizations have nowhere to start [3]. As COBIT hardly covers information security management, ISO/IEC 27001 is better to ensure this aspect. The best option to meet the ISS-GOV in terms of risk management, security, IT governance is to merge COBIT, ISO/IEC 27001, and to manage IT services, ITIL is positioned first in this respect. The combined use of ITIL, ISO 27001 and COBIT standards seems to be the right solution at this stage. This paper is organized along the following lines: Section 2 is devoted to related work in the field. Section 3 provides an overview of the theoretical background of this research, in section 4, authors define the research methodology followed, including data collection, results and analysis, section 5 assesses the obtained results, propose and design a new ISS-GOV model. Conclusion and future work are presented in section 6.

2 Related work

Nowadays, many organizations have come to realize that information security is more than a technical concern [23], Whitman and Mattord have defined information security as "the preservation of the confidentiality, integrity and availability of information and its fundamental components, including the software and hardware that are used to store, process and transmit this information, in a way that is in accordance with security policies, technology, by educating and raising awareness among all personnel involved [24]. Leaders realize that effective and efficient IT security now requires ensuring the confidentiality, integrity and availability of information assets under four dimensions: technical, physical and organizational, as well as managerial. This paradigm change has moved information security to a higher level in terms of business management as a corporate-wide issue. Information security has become a business issue. The organization and its employees are expected to use all available resources to address security risks and to integrate information security into business processes [23]. The inclusion of the latter in C-GOV processes can provide the opportunity to deeply involve stakeholders, an important factor in the protection of critical infrastructures [25, 23]. ISS-GOV is an integral part of C-GOV related to information systems security. Allen has defined corporate security governance as the process of directing and controlling an organization to establish and maintain a culture of security, the aim being to ensure adequate security as a non-negotiable requirement for companies" [25]. Ensuring effectiveness of ISS-GOV, a framework is needed, in this sense, the authors distinguish many frameworks designed and implemented, such as COBIT devoted to IT-GOV and management, although it addresses security in its fifth version it is more focused on IT audit and assessment of the maturity of governance processes. ITIL focuses on IT service management from strategy, design, transition, operation and day-to-day incident management, until to improvement and maintenance. It is, therefore, the reference framework for the delivery and IT management [14]. The ISO 27001 standard defines information security management system requirements, and many of these are met by the implementation of ITIL [20]. Authors also identified some proposed combinations from the literature that are unfortunately neither tested nor converted to a Framework [28]. At this level, it should clear that there is no one single model of practice defined for the ISS-GOV. The risk profile, objectives and procedures of each organization in terms of security are very different, even within the same sector of activity. Significantly, it is important to recognize that any existing model

must be customized or combined with other models to adapt it to the organization's requirements. That is why ITIL, ISO 27001 and COBIT seem the best combination to design a new ISS-GOV model for the governance and management of the ISS from start to finish.

3 Theoretical background

To perform this study, several frameworks and references of best practices are applied to the construction of author's desired output. With this in mind, authors will organize them according to their positioning in the organization, and then they will choose the components of desired findings. As long as the main objective is a customized model for ISS-GOV, it is natural to choose COBIT (IT-GOV and audit side), ITIL (IT service management side), ISO 27001 (information security side) and PDCA (continuous improvement perspective). An overview of the components, to show the consistency and effectiveness of the choice, then a qualitative study based on the experts' judgment in order to select the relevant controls and validated processes. In the end, designing the desired output and measure it with a maturity grid.

3.1 COBIT

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for IT governance and management that was created in 1992 by both the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). COBIT is primarily published and used by the IT community. In the meantime, management guidelines have been introduced and COBIT became the internationally adopted framework on IT governance and control [10] [26]. COBIT provides IT managers, auditors and end-users with a set of commonly accepted metrics, indicators, processes and best practices that can help them to maximize the advantages of using IT and develop the appropriate IT governance as well as control within a company. In its most recent edition, COBIT contains 37 high-level objectives covering 215 controls objectives categorized into five areas below, four of them dedicated to IT management and the fifth one to the IT-GOV, as shown in the following table (Table 1):

1. APO: Align, Plan and Organize.
2. BAI: Build, Acquire and Implement.

3. DSS: Deliver, Service and Support.

4. MAE: Monitor Evaluate and Assess.

5. EDM: Evaluate, Direct and Monitor.

PDCA	COBIT	Processes orientation	Processes number
PLAN	APO	IT management	13
DO	BAI, DSS		6
CHECK	MEA		3
ACT	EDM	IT Governance	5

Table 1: Number of COBIT processes by type and its alignment with the PDCA approach

COBIT's mission is to investigate, develop, promote and communicate a set of internationally accepted, updated and authoritative information technology control objectives for the day-to-day use of management and auditors. COBIT's development benefits managers, auditors and users by helping them understand their IT systems and deciding the level of security and controls needed to preserve their business' assets by developing an IT-GOV model.

3.2 ITIL

Information Technology Infrastructure Library (ITIL) is a Framework of best practices of IT service management, introduced and published by the United Kingdom's Office of Government Commerce (OGC), and encompasses all parts of an organization's IT infrastructure[11]. The ITIL systematic approach to managing IT services can help organizations better understand risk management, enhance relationships with customers, establish profitable practices and ensure a stable IT environment for growth, expansion as well as for change. It is iterative, multi-dimensional and in the form of cyclical process structure, it adopts an integrated approach as required by the ISO/IEC 20000 standard [12]. ITIL is now the worlds best-accepted IT service management approach [13]. It has been subject to a number of revisions over its history and now comprises five books, each one covering a stage of the IT service lifecycle. Its publications are as detailed below [14]:

(1). IT Service Strategy (SS): It provides guidance in how to plan, design, develop and deploy IT services according to organizational capacities and policy assets.

(2). IT Service Design (SD): It provides a roadmap and guidelines for designing and developing services and processes for service management.

(3). IT Service Transition (ST): provides guidance regarding the manner in which coded service strategy requirements in service design are actually met in the operations of the services while mitigating the risks of failures and disruptions.

(4). IT Service Operation (SO): The main purpose is to make certain that IT services are effectively and efficiently delivered, this is where the value is generated , in the same time the services are made functional.

(5). IT Continual Service Improvement (CSI): As with any quality approach, ITIL does not deviate from the rule, during this stage, implementers have to adjust deviations, as well as improve and maintain them.

ITIL describes the processes, functions and structures supporting the IT service management domains, particularly from the service provider perspective. In its approach, it outlines management of information security processes [15].With information security management (ISM) positioning on service management, "service design", this process is incorporated into several other processes that more easily streamline the ISM process in the service life cycle [16].
The principal goal of the ISM process is to align IT security with business security and ensure that information security is effectively managed in all service and service management activities. The ITIL security management process describes the structured fitting of security in the management organization; this process is based on the ISO 27001 standard [17].
The ISM process contains several sub processes in ITIL v3. They are design of controls, testing, incidents management and security review. The objective of the sub-processes of the security controls is to design the appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of an organizations assets, information, data and services [14].

ITIL 2011 includes 26 processes scattered over each phase of the lifecycle service as mentioned in Table 2.

3.3 ISO 27001

ISO / IEC 27001: 2013 [20] is the international standard for entities to manage their information security. It expose how a company should ac-

Phases	Number of Processes
SS	5
SD	8
ST	7
SO	5
CSI	1

Table 2: ITIL 2011 phases and corresponding number processes

commodate the requirements of information security namely, confidentiality, integrity and availability of its information assets and incorporate that into an ISM [17]-[11]; it specifies requirements for the establishment, implementation, operation, monitoring, revision, maintenance and improvement of ISMS documented within an organization. It is designed to ensure the selection of adequate and proportionate security controls to protect information. This standard is generally applicable to all types of organizations. The standard introduced a cyclical pattern known as "Plan-Do-Check-Act" Model (PDCA) that aims to establish, implement, monitor and improve the efficiency of an organization's ISMS system.
The first clauses constitute the introduction (object, references and glossary); Clauses 6 to 10 are the important clauses of the standard. The application of these five clauses is mandatory to establish effective ISMS.

Clause 4 - Context of the organization: understanding the organizational context, the needs and expectations of interested parties and defining the scope of the ISMS. This clause states very plainly The organization shall establish, implement, maintain and continually improve the ISMS.

The ISMS implementation is based on the PDCA quality method as below [18] [19]:

Clause 5 - Leadership: indicates that management must demonstrate commitment and must provide all necessary resources (material, human, financial) for the implementation of ISMS, and it is transversal with all the other phases.

Clause 6 Planning: establishing the ISMS Phase: demonstrates the importance of conducting internal audits at regular intervals to ensure that the ISMS implementation is effective and meets defined objectives;

that the processes and procedures of this ISMS comply with the ISO 27001 standard but also applicable legislation or regulation.

Clause 7 Support: requires the conduct of reviews (at least once a year) to ensure that the ISMS is adequate, compliant and effective. During these reviews, the results of the ISMS internal audits are reviewed and corrective and preventive actions are defined.

Clause 8 operation, implementing and exploitation of the ISMS phase: allows the organization to verify that the actions implemented are effective over time. This is done through audits, event analysis, corrective and preventive actions and reviews.

Clause 9 Performance evaluation: monitoring and review of the ISMS Phase: Evaluate and, if needed, assess the performance of the process according to the ISMS policy, objectives and practical aspects, and report the results to management for review.

Clause 10 Improvement: Maintain and improvement of the ISMS phases: Take corrective and preventive measures, based on the results of the ISMS internal audit and the management review or other relevant information in order to improve the ISMS [13].

3.4 PDCA

PDCA (Plan-Do-Check-Act) is an iterative, four-stage, approach for continually improving processes, products or services, and for resolving problems [21].
The constant change of the business, technology and society requires a continuous assessment process of the effectiveness and efficiency of all ISS controls and the adaptation of the information system to changing requirements.
The outcome is the control loop the PDCA model [22]:

PLAN: Plan and implement ISS processes and controls;

DO: Perform ISS checks;

CHECK: Monitor the implemented ISS processes and controls;

ACT: Initiate the needed change of the ISS system.

4 Research methodology

The authors conduct an exploratory study with experts to set up a series of COBIT 5, ITIL 2011 processes and ISO 27001: 2013 controls to define the ISS-GOV model. To do this, authors apply the Delphi approach [27, 28], aims to select a set of processes that experts have estimated as easy, important and most commonly used.
The Delphi method aims to highlight convergences of opinion and to reach consensus on specific subjects, often with a significant prospective character, by consulting experts using a range of questions [5].
The method is composed of two sub processes, namely the expert selection process (phase1, phase 2) and the questionnaire administration process (phase 3, phase4, phase 5) Fig. 1. These phases are covered all along this paper:
In order to analyze the data for consensus and divergence, we opted for the following measures: For each expert, these numerical responses are entered into a spreadsheet that will calculate descriptive statistics:

Me: The median of each proposal;

EAM: The absolute deviation from the median;

Using the following equation:

$$EAM = \frac{\left|\sum_n^i X_i - M\right|}{n} \tag{4.1}$$

Xi: Degree of the proposal appreciated by the expert i;

M: Median of the proposal;

n: Total number of experts.

To measure the degree of consensus or divergence for each process and control, it is possible to use a threshold EAM, an EAM less than or close to 1 synonymous with consensus [6, 7] and/or to analyze the dispersion of the responses:
%IIQ: the percentage of responses in the range [q1; q3];
The Delphi study is going to cover 1 main question, with 3 groups of questions:

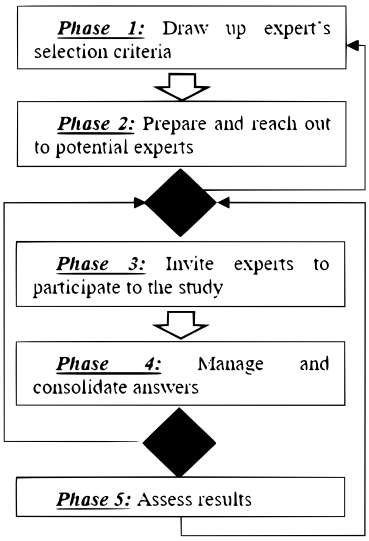

Figure 1: The customized Delphi method

Q1: practices and processes related to IT governance, IT service management, and information security can be integrated into a single model providing a homogeneous ISS-GOV framework?

Q2: ITIL: which processes ensure implementing IT Service Management (in terms of cost, ease of use and implementation), covers 175 questions covering all service life-cycle processes.

Q3: ISO27001: which controls ensure the correct level of security of IT infrastructures (in terms of cost, ease of use and implementation)? Covers 123 questions about the different security controls.

Q4: COBIT: which processes implement easily IT governance (in terms of cost, ease of use and implementation)? Covers 37 questions covering the different processes of IT-GOV.

4.1 Data collection

The choice of experts is a crucial step that influences the quality of the results [8, 9]. As this is not a simple opinion survey, the validity of the results of the Delphi method does not depend on sampling but on the knowledge, skills and, above all, the intentional cooperation of the experts consulted;

therefore, the choice is based on the professional field of the expert, the duration of experience in IS security, IT management and IT governance, and the number of projects conducted in the said fields; the professional field can be broken down into different statuses, in particular : security managers, analysts, IT project managers with more than 10 years of experience in the implementation of security systems, IT service management and IT projects. The main reason why this study is limited to professional IT practitioners is the fact that the concepts of security management, service management and IT governance require a very solid feedback in the field, as well as a mature background through practice.
we used LinkedIn to select the experts, in which the different profiles containing details of both academic and professional career paths, the various positions held with the corresponding duration's, the list of IT projects conducted as well as the list of IT certifications, after browsing through LinkedIn more than 100 profiles that corresponded to the established criteria, a list of 76 experts was drawn up on a Word document containing the confidential number assigned to the expert to guarantee his anonymity, e-mail address, function, company name, telephone number and country of residence.
We reached the experts listed in step 2 by LinkedIn online messenger, when they express their collaboration and willingness to participate in our study, we move on to step 3. Of the 76 potential experts targeted, 18 of them, from 13 countries (England, Australia, Morocco, Canada, United States, Spain, Estonia, Finland, Hungary, India, Portugal, Switzerland, Thailand) accepted to participate in our Delphi survey, therefore the validation condition required by the Delphi method is met with this number of participants. The third step involves inviting each of the 18 experts to participate in our survey by explaining the objectives of the study, the procedures to be followed and the duties associated with their participation in order to ensure the success of the study. We asked each participant to use e-mail to receive or send the questionnaires and responses. All participants chose e-mail as a tool for correspondence.
In Steps 5, 6, we asked the experts to give their opinion on the following items:

1. The links that may exist between the concept of IT security management (ITSecM), IT service management (ITSM) and IT governance (IT-GOV), with the aim of determining the feasibility of designing an integrated 3-in-1 model for ISS governance;

2. the most commonly used ITSM, namely the processes of the 5 phases

that constitute the service lifecycle described in the ITIL repository;

3. the most widely used IT-GOV processes, in this case the COBIT processes;

4. the most impacting security controls of the enterprise architecture, in this case those described in the ISO27001 standard.

Three rounds of the Delphi survey were necessary to reach a consensus on the main question as well as the 3 other categories of questions. The first round consisted in performing a preliminary survey among all the experts chosen for the study. Once this first survey has been carried out, the same survey is repeated, with the same experts, but with the results of the first survey. During this second round, each expert can see, anonymously, how the others responded, and can either maintain his or her response or decide to move closer to the general opinion. Three rounds of surveys have led to the decision that a consensus has been reached.
The first round of the questionnaire, which took place from 1 January to 18 February 2019, consisted in defining the key concepts of information security governance, as well as the processes and controls ensuring the 3 disciplines, ITSM, ITSecM and IT-GOV.
In the first round, the questions were developed and presented to the experts taking into account the links that could exist between ITSM, ITsecM and IT-GOV. Once the three rounds of the main question were completed, it became possible to move on to the second round where three additional categories of questions were added, namely 175 questions on the processes that ensure ITSM, another category of 37 questions on the processes most used to ensure good IT-GOV and the third of 123 on the most used security controls (ITSecM). In order to assess the degree of consensus of participants, we adopted and personalized the Likert scale [29], which includes 6 answers: Strongly agree (6), agree (5), somewhat agree (4), neutral (3), disagree (2) and strongly disagree (1); each expert had to provide one of these answers according to his experience.

4.2 Results and discussion

"This study defines the concept of information systems security governance, through 3 dimensions, namely ITSM, ITSecM, and IT-GOV."

Q1: practices and processes related to IT governance, IT service management, and information security can be integrated into a

single model providing a homogeneous ISS-GOV framework?

The results of the first round showed the degree of consensus on the 3 disciplines that may comprise ISS-GOV. The results were almost similar or even more convincing for the 3 Delphi rounds, as shown in the table (table 3) below:

Q1	*E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18	M	EAM	Error(%)
Tour1	4	5	4	3	5	3	5	3	3	3	5	5	6	3	5	4	5	5	4.222	1.003	23.761
Tour2	5	6	5	4	3	5	4	4	4	4	5	4	5	5	6	5	6	5	4.722	0.826	17.501
Tour3	5	6	6	6	6	6	5	4	5	5	5	5	6	5	6	5	6	6	5.444	0.616	11.309

Table 3: experts' answers in all three rounds for Q1 (*E=Expert)

With consensus: $4 < Me < 7$ $0.6 < EAM < 1$
Without consensus: $3 < Me < 5$ $1,1 < EAM < 1,8$

Which leads to the following measurable consensus results:

	Me	EAM1	EAM2	EAM3	IM1%
Q1	4.8	1	0.82	0.61	76%
Q50	3.3	1.79	1.55	1.31	46%

Table 4: Consensus reached around the 3 ISS-GOV disciplines of the 3 rounds

The statistical analysis revealed two main groups of processes: Q1 which has consensus (rather strong median between 4 and 7, with small deviations from the median between 0.6 and 1) and Q50 (corresponds to the supplier management process of the ITIL Service Design Phase) has disagreement (weak medians between 3 and 5, with strong deviations from the median between 1.1 and 1.7). The table above gives the example of the figures for Q1 (with consensus) and Q50 (without consensus). Following the consensus of Q1, it was concluded that the 3 disciplines can be integrated into a unified ISS-GOV framework, therefore the design of this integrated model is now possible; containing these three dimensions, while keeping the processes that have consensus and eliminating those that converge; it remains to determine the processes and controls that are components of the latter. To do this, we have proceeded in the same way of questioning for each discipline (3 turns for each concept), as shown in Q50 corresponds to the process "supplier management" which, its degree of consensus is low.
To do this, we proceeded in exactly the same way of questioning each discipline (three rounds of interviewing for all questions in each category). In the panel of 335 questions distributed as follows (table 5):

	ISO 27001	COBIT	ITIL
Initial number of questions	123	37	175
With consenus	23	10	12
Without consensus	100	27	153

Table 5: Final results of all processes and controls

Based on the table above, the questions with consensus will constitute the new ISS-GOV model as shown in Table 7.

5 Proposal: ISS-GOV integrated model

5.1 Merging of ITIL, COBIT, ISO27001 with PDCA approach

At this level, the authors can merge the processes and controls (ITIL, COBIT and ISO 27001) validated by the experts into a single ISS-GOV approach.
The following table (table 5) shows the correspondences of each standard and Frameworks, removing redundancies, overlaps and completing missing parts, and this while being aligned with continuous improvement.
The proposed ISS-GOV model refers to a systemic approach by which an organization ensures the safety of it IS in an agile manner.
To set up the proposed model, implementer may use the following table (table 6):

5.2 CONCEPTUAL MODEL OF ISS-GOV

To simplify the implementation of the ISS-GOV model, its design is necessary because it describes the different phases with the corresponding outputs and highlights the cyclical phase sequence. To do this, BPMN seems to be better because it models both IT and business process, Fig.2 illustrates the conceptual model mentioned below:

The above conceptual model represents the 5 phases of the new hybrid approach of the ISS-GOV. A process represents each phase, since it contains multiple tasks as indicated in Table 6; the output of each phase represents the input of the second one. As the approach is in alignment with the PDCA (continual improvement), if shortcomings are found at the planning stage, implementer can return to correct and then terminate the loop. The various

Phase	Processes and controls
Phase1: **Establish ISS-GOV**	**APO 02** Manage Strategy **APO 06** Manage Budget and Costs **APO 03** Manage Enterprise Architecture **SS** Financial management for IT services
Phase2: **Build and implement ISS-GOV**	**BAI 02** Manage Requirements Definition **BAI 01** Manage Programs and Projects **BAI 05** Manage Organizational Change Enablement **SD** Service level management **SD** Availability management **SD** Capacity management **SD** IT service continuity management **MC, OC, BP** and **TC** implementation.
Phase3: **Operate and support ISS-GOV**	**ST** Change management **ST** Release management **ST** Configuration management **SO** Incident management **SO** Problem management **SO** Service desk
Phase4: **Monitor and review ISS-GOV**	**EDM 02** Ensure Benefits Delivery **EDM 01** Ensure Governance Framework Setting and Maintenance **EDM 03** Ensure Risk Optimization
Phase5: **Maintain and improve ISS-GOV**	**MEA 01** Monitor, Evaluate and Assess Performance and Conformance

Table 6: ISS-GOV model phases and corresponding tasks

Deliverable are symbolized with the database and the acronyms are explained in the table below (Table 7).

6 Conclusion

Nowadays, in every organization, IT services have to be provided in a cost-efficient way, mitigating security threats and conforming to legal and regulatory requirements. The equation is challenging to solve and, in some instances, it may seem impossible. To survive in this environment, the proposed ISS-GOV model in the form of an in-house repository, seems appropriate for this purpose. Now implementer have one framework for implementing IT

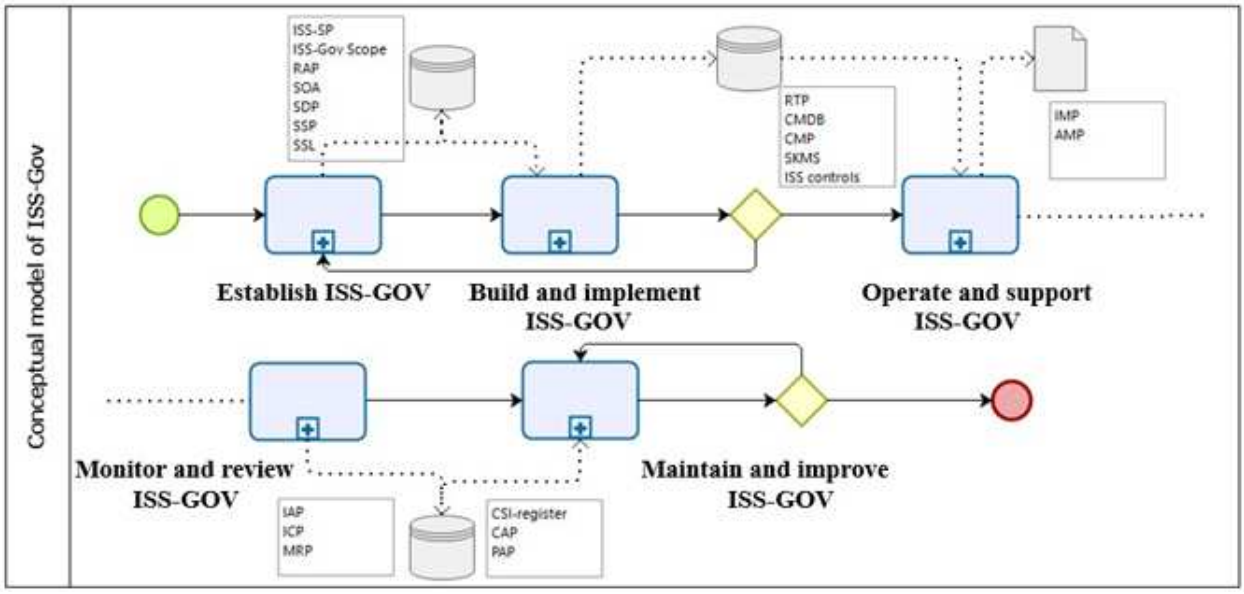

Figure 2: ISS-GOV conceptual model

strategies, plans and processes, for defining metrics, benchmarks and audits, and for integrating security issues to reduce risk. For future work, we plan to adopt our model through a case study to prove its effectiveness.

ISS-GOV conceptual model	
Phases	**Outputs**
Establish ISS-GOV	ISS Service policy (ISS-SP) ISS-GOV scope Risk assessment process (RAP) Statement of applicability (SOA) Service design package (SDP) Service strategy plan (SSP) Service level agreement (SSL) ISS continuity plan (ISS-CP) ISS availability plan (ISS-AP)
Build and implement ISS-GOV	Risk treatment process (RTP) Configuration management database (CMDB) Change management process (CMP) Service knowledge management system (SKMS) ISS controls
Operate and support ISS-GOV	Incident management process (IMP) Access management process (AMP)
Monitor and review ISS-GOV	Internal audit procedure (IAP) Internal control procedure (ICP) Management reviews procedure (MRP)

Table 7: ISS-GOV conceptual model outputs

References

[1] K. J. Knapp, R. F. Morris Jr., T. E. Marshall, T. A. Byrd,*Information security policy: An organizational-level process model,* Computers and Security,**28,** no. 7, (2009), 493–508.

[2] S. De Haes, W. Van Grembergen,*Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value Featuring COBIT 5*, Springer Verlag, New York, 2015.

[3] S. Sahibudin, M. Sharifi, M. Ayat. *Combining ITIL, COBIT, and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations*, (2018), 1–5.

[4] ISACA (Information Systems Audit and Control Association), COBIT 5 *Un réfèrentiel orient affaires pour la gouvernance et la gestion des TI de lentreprise*, A Business Framework for the Governance and Management of Enterprise IT, 2012.

[5] N. Dalkey, O. Helmer, *An experimental application of the Delphi method to the use of experts*. Management science, **9,** no. 3, (1963), 458–467.

[6] C. C. Carpenter, D. A., Cooper, M. A. Fischl, J. M. Gatell, B. G. Gazzard, S. M. Hammer, D. D. Richman, *Antiretroviral therapy in adults: updated recommendations of the International AIDS SocietyUSA Panel*. Jama, **283,** no. 3, (2000), 381–390.

[7] E. Zenou, *Comment intégrer la valeur crée par le dirigeant dans la valeur crée par l'entreprise: contribution à la connaissance de la valorisation du dirigeant: une application sur le marché francais*, Doctoral dissertation, Lyon 3, 2004.

[8] M. Adler, E. Ziglio, *Gazing into the oracle: The Delphi method and its application to social policy and public health*, Jessica Kingsley Publishers, 1996.

[9] F. Bolger, G. Wright, *Assessing the quality of expert judgment: Issues and analysis. Decision support systems*, **11,** no. 1, (1994), 1–24.

[10] E. Lachapelle, *White Paper: Control objectives for information and related technology*, Veridion Inc., Montreal, Canada, October 2, 2007, [Online]. Available: www.veridion.netH\ITIL+COBIT\cobit.en.wp.pdf.

[11] G. Disterer, *ISO/IEC 27000, 27001 and 27002 for information security management*, Journal of Information Security, **4,** no. 2, (2013), 92–100.

[12] R. Sheikhpour, Nasser Modiri, *An approach to map COBIT processes to ISO/IEC 27001 information security management controls*, International Journal of Security and its Applications, **6,** no. 2, (2012), 13–28.

[13] R. M. N. Sheikhpour, N. Modiri, *Mapping approach of ITIL service management processes to ISO/IEC 27001 controls*, Journal of Computing, **37,** (2011), 117–124.

[14] E. R. Larrocha, J. M. Minguet, G. Daz, M. Castro, A. Vara, *Filling the gap of information security management inside ITIL: proposals for posgraduate students*, Proceedings of the IEEE International Conference on Education Engineering (EDUCON2010), April 2010, 907–912.

[15] H. Susanto, M. N. Almunawar, Y.-C. Tuan, *Information security management system standards: A comparative study of the big five*, International Journal of Electrical Computer Sciences, **11,** no. 5, (2011), 23-29.

[16] R. Sheikhpour, N. Modiri, *A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management*, Indian Journal of Science and Technology, **5,** no. 2, (2012), 2170-2176.

[17] A. Rezakhani, A. Hajebi, N. Mohammadi,*Standardization of all information security management systems*, International Journal of Computer Applications, **18,** no. 8, (2011), 4–8.

[18] D.C. Tofan,*Information security standards*, Journal of Mobile, Embedded and Distributed Systems, **3,** no. 3, (2011), 128-135.

[19] Rebollo, Oscar, Daniel Mellado, Eduardo Fernàndez-Medina, *A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment*, J. UCS, **18,** no. 6, (2012), 798–815.

[20] International Standards Organization (ISO), *Information technology security techniques- information security management systems Requirements*, (ISO/IEC 27001, IDT, (2013), 5-32, www.iso.org.

[21] A. Labodovà, *Implementing integrated management systems using a risk analysis based approach*, Journal of Cleaner Production, **12,** no. 6, (2004), 571-580.

[22] T. A. Walasek, Z. Kucharczyk, D. Morawska-Walasek, *Assuring quality of an e-learning project through the PDCA approach*, Archives of Materials Science and Engineering, International Scientific Journal, **48,** no. 1, (2011), 56–61.

[23] B. Khoo, P. Harris, S. Hartman, *Information security governance of enterprise information systems: An approach to legislative compliant*, International Journal of Management and Information Systems, **14,** no. 3, (2010), 49–55.

[24] M. E. Whitman, H. J. Mattord,*Roadmap to Information Security: For IT and Infosec Managers*, Cengage Learning, Aug. 2012, 400 pp.

[25] S. Posthumus, R. Von Solms, *A framework for the governance of information security*, Computers and Security, **23,** no. 8, (2004), 638–646.

[26] S. De Haes, W. Van Grembergen, R. S. Debreceny, *COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities*, Journal of Information Systems, no. 1, (2013), 307–324.

[27] I. P. Booto Ekionea, B. Prosper, M. Plaisent, *Consensus par la méthode Delphi sur les concepts clés des capacités organisationnelles spécifiques de la gestion des connaissances*, Recherches qualitatives, **29,** no. 3, (2011), 168–192.

[28] C. Okoli, S. D. Pawlowski, *The Delphi method as a research tool: an example, design considerations and applications*, Information and management, **42,** no. 1, (2004), 15–29.

[29] B. P. Subedi, *Using Likert type data in social science research: Confusion, issues and challenges*, International journal of contemporary applied sciences, **3,** no. 2, (2016), 36–49.