2021 Research, Invention, and Innovation Congress: Innovation Electricals and Electronics (RI2C) | 978-1-6654-0300-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/RI2C51727.2021.9559772

Guidelines for Information Technology Governance Based on Integrated ISO 38500 and COBIT 2019

Busarin Visitsilp
Department of Information Technology
King Mongkut's University of Technology North Bangkok,
Bangkok Thailand
s6307011910529 @email.kmutnb.ac.th

Nalinpat Bhumpenpein
Department of Information Technology
King Mongkut's University of Technology North Bangkok,
Bangkok, Thailand
nalinpat.b@itd.kmutnb.ac.th

Abstract—**Information technology has become an integral part of the main task enhancing organizations success. The results are in line with the goals set by many organizations, both in the government and private sectors, for a better recognition of the significance on information technology work and initiation of viewpoints on information technology governance. This research proposes the concept of adopting an integration of ISO 38500: 2015, an international standard for information technology governance, and guidelines recommended for the executive committee on an effective and acceptable implementation of information technology within the organization, and COBIT 2019 framework via mapping the 6 key principles of information technology governance of ISO 38500: 2015 and the 5 domains and 40 processes of COBIT 2019 core processes through a consideration of the processes relevant and suitable for the organization's context as a case study for the guidelines on information technology governance and a determination on operational guidelines conformity with the organization's objectives to achieve the desired benefits and goals.**

Keywords—component, IT Governance, ISO 38500; COBIT 2019; Maturity Assessment

I. Introduction

Information Technology (IT) plays an essential role in every organization to help drive strong businesses and operations for an edge over competitors in the same industry. In order to establish effective operations, Information technology needs to be aligned with the organization's business strategies. One of them enhancing technology management is IT Governance (ITG) [1]. However, many organizations still lack of corporate governance in information technology. This may be caused by several reasons; for example, that the senior management committee still lacks of an understanding of information technology limits the recognition on the significance of information technology resulting in damages and impacts to the operations including that the work results are unable to meet the organization's objectives. Therefore, Information technology governance will help organizational leaders recognize the significance and necessity of information technology's objectives to be aligned with corporate strategies as well as the essentiality of governance in order to increase the management efficiency of information technology which is another driving part for the organization to achieve the goals and objectives planned.

In the past, information technology management frameworks have been applied to improve operational strategies to uplift organizational efficiency by adopting COBIT, a recognized international information technology management framework. COBIT or Control Objective for Information and Related Technologies [2,3] is an information technology management framework for the purposes of data and related technologies control, risk management, and IT activity governance. In addition to the framework applied as a guideline for decision planning to define rules and regulations appropriate for the organization strategies and goals. The application of information technology standards encourages more efficient IT governance. ISO 38500 is an international standard for information technology governance [4] with explicit principles and topics relating to IT governance which enhancing understandings of committees and top management on the principles guidelines of rules and regulations determination for IT operation governance of the organization.

This research aims to integrate the principles of ISO 38500: 2015 and COBIT 2019 for guidelines on information technology governance in order to enhance conformance between information technology and business operations, including allowing the board, senior management, and stakeholders of the organization to recognize the significance and benefits of information technology governance. This is for the organization's achievement on the goals established. This research has conducted a case study from a state enterprise.

II. Related Work

This section provides an overview of the IT governance approach with an integration of ISO 38500 and COBIT.

A. ITG (Information Technology Governance)

ITG is the governance of information technology, which is the responsibility of the board, senior executives, and executives in information technology to demonstrate vision and leadership in supporting technology operations to achieve goals according to the strategies and objectives planned [5]. ITG principles are increasingly being used in a wide range of businesses and services. ITG has been applied to assist in information technology governance and Cloud security procedures (cloud computing) which requires IT governance to manage risks and ensure that IT work and

978-1-6654-0300-9/21/$31.00 ©2021 IEEE

Cloud computing will increase the business value of the organization [6].

B. ISO 38500

ISO 38500 is an international standard for corporate governance in information technology and provides advice to senior management committees on the efficient and acceptable implementation of information technology within the organization. Currently, ISO 38500: 2015 [7] contains six principles of IT Governance [8].

- Responsibility
- Strategy
- Acquisition
- Performance
- Conformance
- Human Behavior

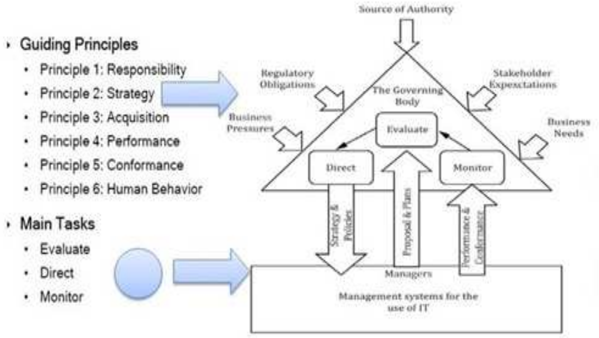


Fig.1 ISO38500:2015 Model

The implementation of ISO 38500 can be conducted in combination with any other standards or frameworks. Nowadays, information is a priority for all organizations that the protection of information security services, including confidentiality, completeness, and availability needs to be recognized. There is a research addressing an integration of ISO 38500 and ISO 27001, the international standards for information security management, along with ITIL, the best practice framework for IT services. When the three standards are in collaboration, it enables an integration of the best security practices of IT governance assisting organizations reduce the cost of acceptable security-level maintenance and effectively reduce the level of general risks. Therefore, it can be concluded that practices using ISO 38500, ITIL, and ISO / IEC 27001 can better control information security [9].

C. COBIT

COBIT (Control Objective for Information and Related Technologies) is an information technology management framework supporting the development, organization, and implementation of strategy on information technology management and governance. The development has been evolving since 1998 until now as the COBIT 2019 edition [2], which has been updated on the cooperate framework based on emerging technology trends. It presents the concepts emphasizing on corporate governance of information technology in specific areas such as cyber security, digital transformation, cloud computing, [2] etc.

Many organizations have applied COBIT as an addition to their business value. In tertiary educational institutions, COBIT has also been applied. There are researches mentioning the integration of COBIT 5 with ISO 38500 in order to acquire good IT governance practices through a collaboration of ISO 38500 standard and COBIT 5 framework to determine factors affecting IT governance. It was found that ISO 38500 can effectively interpret corporate vision and mission with the contributing factors of COBIT 5 [10]. The ISO 38500 standard is in collaboration with the COBIT 5 framework to shape job alignment on governance and efficiency measurement by applying the six principles of ISO 38500, paired with COBIT 5. It was found that IT management has improved for better standards and efficiency [11].

D. Literature Review

An example of previous research involves the integration of ISO 38500 with COBIT which is a case study conducted in a tertiary educational institute. Nugroho and Surendro [10] work applied ISO 38500: 2008 and COBIT 5 through an analysis of ISO 38500 framework whether its objectives or goals matches with the organization. Then, a consideration of COBIT 5 active features is made for the best practices possible for a corporate strategic plan. However, there has not been an assessment to generate an organizational model for job positioning on IT governance. As same as the work of Widjajanto, Santoso, and Rijati [11], a research was conducted on modeling creation, quality assurance system placement, and measurement of tertiary institutions' performance using ISO 38500: 2008 and COBIT 5 by establishing business goals, identifying IT goals, determining IT procedures and locating processes. After that, the process model of COBIT 5 was considered and optimized with the 6 IT Governance Principles of ISO 38500. It was found that the competence level of most IT processes was at level 1, and therefore, a standardization and performance measurement index should be carried out.

As an example of the research discussed above, ISO 38500 is selected in conjunction with COBIT 5 to determine best practices in organizational strategic planning or consider for the optimal IT positioning in line with business goals. Regarding this research, the researcher has selected an application of ISO 38500: 2015 standard and COBIT 2019 by matching the six fundamental principles of ISO 38500: 2015 IT governance with the 5 domains, 40 processes of COBIT 2019. A design of assessment practices on processes and maturity of the organizational IT governance through activities suggested by COBIT 2019 document [2].

III. Methodology

Based on relevant research studies on information technology governance guidelines, it was found that the COBIT process was integrated with ISO 38500, an international standard for information technology governance, has assisted committees and top management understand the principles of rules and regulations establishment guidelines regarding IT operational governance of the organization. In this research, COBIT 2019 was selected in integration with ISO 38500: 2015 by cooperatively considering the six principles of ISO 38500 together with the regulatory system components of COBIT 2019, detailed in Fig.2.

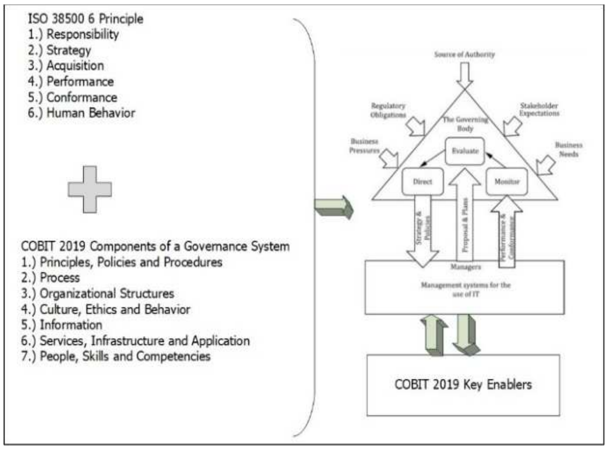


Fig.2 ISO 38500: 2015 and COBIT 2019 Key Elements

A. ISO 38500:2015 and COBIT 2019 Process Mapping

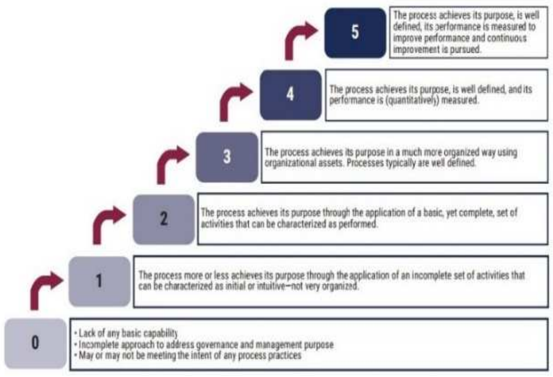
To obtain guidelines for information technology governance appropriate for the organization's context used as a case study, an application of the six principles of ISO 38500: 2015 standard, combined with the COBIT 2019 processes was implemented. The selected COBIT 2019 procedures are as follows:

Table I. Process Mapping

ISO38500 Principle	**COBIT Process Domain**				
	EDM	***APO***	***BAI***	***MEA***	***DSS***
1. Responsibility	EDM05	-	-	-	-
2. Strategy	EDM01 EDM02	APO01 APO02			
3. Acquisition	-	APO05	-	-	-
4. Performance	-	APO02 APO09	BAI04	MEA01	-
5. Conformance	-	APO02	-	MEA01 MEA02 MEA03	-
6. Human Behavior	-	APO07	BAI05 BAI08		-

B. Assessment Approach

Process Performance Management in COBIT 2019 (COBIT Performance Management: CPM) is an integral part of the information technology governance system in COBIT 2019. Performance Management consists of CMMI-based process capability assessment model providing 5 capability levels scores from 0 – 5. In COBIT 2019, each process assessment was conducted deeper into the activity level of that process. The details of each competence level are shown in Fig.3 [12].



The process achieves its purpose, is well defined, its performance is measured to improve performance and continuous improvement is pursued.

The process achieves its purpose, is well defined, and its performance is (quantitatively) measured.

The process achieves its purpose in a much more organized way using organizational assets. Processes typically are well defined.

The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed.

The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive—not very organized.

- Lack of any basic capability
- Incomplete approach to address governance and management purpose
- May or may not be meeting the intent of any process practices

Fig. 3 Capability Levels for Process [12]

Previous research reviews have suggested CMM 1.1 evaluation approach, which Motorola had conducted a trail and succeeded [13]. Therefore, this research has applied the assessment approach in 3 areas: Approach, Deployment, and Result by scoring with a total of 6 levels. An increase of a 2- point-score is added in each level as follows.

- Level 1 no action, improvement needed, 0 point
- Level 2 improvement needed, 2 points.
- Level 3 fair, 4 points.
- Level 4 good, 6 points.
- Level 5 very good, 8 points.
- Level 6 excellent, 10 points.

The scoring can be considered as an odd number, for example, 5 points, 7 points, depending on the assessor's consideration if it is found that in the area being assessed, there may be only some parts that have not been implemented resulting in incomplete criteria met. The perfect score of each area is 10, so the perfect score of each activity is 30 points. Then, the score in each area obtained was calculated for an average. After an assessment and grading in each area, the concerned departments are able to set appropriate criteria or averages to promote competency to the higher levels. In this research, the grading scores for each process were considered, and the average score in each area required was seven or more points to be considered for the higher level.

C. Case Study

This research evaluates the proposed guidelines for information technology governance based on integrated ISO 38500 and COBIT 2019 through a case study at the Information Technology Division of a state enterprise in February 2020, with three participants of senior executives involved in the assessment. This state-owned enterprise operates in the telecommunications industry providing telecommunication infrastructure and digital services.

IV. Result

The activity assessment and grading results in each level of each COBIT 2019 process conducted on the case study demonstrated that the points of all levels in each process evaluated scored less than the average of 7 points as the evaluation criterion established.

Table II. Assessment Result

COBIT 2019 Process	**Process Name**	**Avg. Score**
EDM (Evaluate, Direct and Monitor)		
EDM01	Ensured governance framework setting and maintenance	3.19
EDM02	Ensured benefits delivery	3.59
EDM05	Ensured stakeholder engagement	4.73
APO (Align, Plan and Organize)		
APO01	Managed IT management framework	4.06
APO02	Managed strategy	3.42
APO05	Managed portfolio	3.25
APO07	Managed human resources	4.45
APO09	Managed service agreements	5.61
BAI (Build, Acquire and Implement)		
BAI04	Managed availability and capacity	5.50
BAI05	Managed organizational change	4.78
BAI08	Managed knowledge	4.69
MEA (Monitor, Evaluate and Assess)		
MEA01	Managed performance and conformance monitoring	4.25
MEA02	Managed compliance with External Requirements	3.24

. Referring to the scores of each selected process activity graded at level 2, it was found that the average score in each process was lower than 7 points, which resulted in failing the assessment criteria for higher levels. Since the scores perceived in level 2 has not yet met the assessment criteria for the perception of IT Governance Guidelines, it was not required for level 3 - 5 assessments. However, the organization will need to review for level 2 activity learning and development of the selected processes in order to be achieved and be able to progress to the higher levels.

Therefore, this research has proposed the more efficient information technology development and governance guidelines as follows: 1) to study the organization's limitations in details in order to be able to select processes, approaches, and practices appropriate for the organization, and 2) to study the operational perspectives with a consistency between information technology activities and business operations since the objective of information technology governance is to enable collaborations of information technology and business operations in order to support the corporate strategies and goals. Therefore, a study on information technology and other work gaps should be conducted in order for the improvement and development of the problems encountered on appropriate approaches and practices for further efficient and effective outcomes.

V. Conclusion

This research is a study of corporate governance practices in information technology with a combination of ISO 38500: 2015 and COBIT 2019 of a state enterprise to assist the board and senior management of the organization recognize the significance of the information technology work which is nowadays regarded as an important operational part supporting the organization’s achievement according to the set goals. In this regard, information technology work cannot be solely carried out, but it needs to be aligned with other organizational strategies as well.

This research matched the processes of the COBIT 2019 framework with the six principles of ISO 38500: 2015. The selection of each process and principle matching from the two standards was based on the corporate objectives and goals in order to acquire proper procedures from the assessment results and the activities grading of each process by the three concerned participants in charge of information technology work. It was found that the means of each process did not meet the assessment criteria set. Furthermore, since the assessed scores of level 2 failed, it can be concluded that the competency level progress on IT governance guidelines is still unattainable.

Based on the evaluation results on IT governance guidelines of a state-owned enterprise according to ISO 38500: 2015 standard and COBIT 2019, the operating procedures started from a selection of COBIT 2019 process for mapping with the six principles of ISO 38500: 2015 information technology governance with similarities to those researches regarding Quality Assurance System Orientation Model and the Measurement of Higher Education Performance Based on COBIT 5 Framework [11]. There are still some differences in COBIT processes selected since the selection of processes to be matched with the principles of ISO 38500 has been considered based on the appropriateness in terms of a particular organizational context, objectives, and goals. Regarding assessment and rating, this research conducted an in-depth assessment of the activity level required to be performed at each level of each process. This activity-level assessment is regarded less common in research work on IT governance guidelines. In terms of the assessment method on cognitive competence level of IT governance, this research chose a 3-sided evaluation method: Approach, Deployment, and Result, a similar approach to Motorola's work [13]. The results of the assessment are detailed. The results of the assessments obtained can be utilized to determine improvements on methods and processes for better results.

References

[1] IT Governance Institute, Board Briefing on IT Governance, 2nd ed., USA, 2003.

[2] ISACA, COBIT 2019 Framework Governance and Management Objectives, USA, 2018.

[3] H. Steven, G. Wim, J. Anant & Huygh, Tim, “COBIT as a Framework for Enterprise Governance of IT,” Management for_Professionals, in: Enterprise Governance of Information Technology, edition 3, chapter 5, pages 125-162, January 2020. [online]. doi.org: 10.1007/978-3-030-25918-1_5. [Accessed: February 1, 2020].

[4] IT Governance. *“What is ISO/IEC 38500,”* itgovernanceusa.com. [Online]. Available: https://www.itgovernanceusa.com/iso38500. [Accessed: Dec.05, 2019].

[5] IT Governance. *“What is IT Governance.”* itgovernance.co.uk. [Online]. Available: https://www.itgovernance.co.uk/it_governance. [Accessed: Dec.05, 2019].

[6] F. Salman M. and R. Shawon, Ph.D., “Securing Cloud Computing Through IT Governance,” IT in Industry, vol.7, no.1, February 2019.

[7] ISO. *“ISO/IEC 38500: 2015 Information technology – Governance IT for the organization.”* iso.org. [Online]. Available: https://www.iso.org/standard/62816.html. [Accessed: Dec.05, 2019].

[8] S. Rimas, “Governance of IT and cybernetics,” IEEE Conference on Norbert Wiener in the 21st Century (21CW), July 13-16, 2016.

[9] M. Zaydi and B. Nassereddine, “A new comprehensive solution to handle information security Governance in organizations,” In Proceedings of the 2nd International Conference on Networking, Information Systems &amp; Security Association for Computing Machinery, New York, NY, USA, Article 50, 1–5. 2019. [Online]. doi.org/10.1145/3320326.3320382. [Accessed: February 1, 2020].

[10] N. Heru and s. Kridanto, “proposed model of vocational university governance and measurement model by Utilizing the iso 38500 framework and Cobit 5 enabler,” conference: international conference on ict for smart society, 2013.

[11] W. Budi, S. Dewi Agustini and R. Nova Alignment, “Model of Quality Assurance System of Higher Education and Performance Measurement Based on Framework CobiT 5,” International Seminar on Application for Technology of Information and Communication (iSemantic), 2018.

[12] ISACA, COBIT 2019 Framework Introduction & Methodology,USA, 2018.

[13] D. Michael K, “Achieving Higher SEI levels,” IEEE Software, vol.11, issue 4, July 1994, pp17-44. [Online]. https://doi.org/10.1109/52.300079. [Accessed: February 1, 2020].