The Use of ISO and COBIT for IT Governance Audit

Y Aprilinda\(^1\), A K Puspa\(^2\), F N Affandy\(^3\)

\(^1\)Informatics department, Universitas Bandar Lampung, Bandar Lampung, Indonesia
\(^2\)Information system department, Universitas Bandar Lampung, Bandar Lampung, Indonesia
\(^3\)Technical Information department, STMIK Tunas Bangsa, Bandar Lampung, Indonesia

*ayukartikapuspa@ubl.ac.id

Abstract. Along with the growing number of practices in the use of technology for business processes, there is a need for IT governance for the private and government sectors. Company leaders implement IT governance in order to ensure that the investment spent by the organization for IT can provide benefits or optimal value for the organization and reduce the lowest risk possible. In practice IT governance requires standards. There are several standards that are often used the most popular are COBIT and ISO, both of which are known as IT governance best practices, but can any company apply the two standards? In this paper we will discuss the use of COBIT and ISO in corporate governance, the strengths and weaknesses of each standard and the merging of the two standards for more comprehensive governance practices.

1. Introduction
The most significant change that occurred in the technological era was the change in the role of technology that occurred in organizations, if previously information technology was widely used for automation of manual processes, along with the times and complexity of processes in organizations making IT applications more widely used. The IT function extends not only at the operational level but to the strategic level, from analyzing data, forecasting trends to decision making by leaders. In some information technology industries can be competitive resources to differentiate and provide competitive advantage, in some other industries information technology can also be a solution to minimize risk. This causes the use of IT to spread in all lines of business, with a lot of investment, IT governance is certainly necessary in accordance with the organization's business objectives without leaving applicable international standards.

Fox and Zonneveld [1] concluded that in good governance the role of IT Governance is very important. The IT Governance process begins by setting targets for IT, providing initial guidance. After that, an iteration is continually formed, performance is measured and compared to the initial goal, resulting in a directional return from the required activity and a corresponding change in objectives. When goals are the primary responsibility and measure of management performance, it must clearly be developed with good planning so that the targets are affordable and the size describes the goals precisely. And according to Fox and Zonneveld [1], the final reason for IT Governance is important because of the gap between expectations and reality. The leaders always expects management to providing IT solutions with good quality, on time, and efficiently. Increase the utilization of IT provides business value returns and increase the utilization of IT to improve efficiency and productivity when managing risk. The ineffectiveness of IT Governance allows the causes of negative experiences in the use of IT, including: 1. Business loss, damage to reputation or weak competitive position.
2. The deadline is not reached, the cost is higher than the desired expectations.
3. Efficiency and processes have a negative impact on the low quality of IT use.
4. Failure of IT initiatives can bring about promised innovations and benefits.

In practice, the most widely used international standards for IT governance are COBIT and ISO, but not a few also combine these two standards, this is due to the limitations possessed by both. In the next section of this article the literature study will be presented from several articles that use both standards to assess the maturity of IT governance, the limitations of the two standards, the strengths they have to conclusions on the needs of using each standard.

2. Literature Review
The following describes some of the writings that contain the use of COBIT or ISO and articles that contain both standards

2.1. Service Performance Measurement in Semarang City 1 Samsat Using COBIT 5 and Quality Perception Method by Dina [2]
This research is about measuring the performance of internal parties using COBIT 5. The research is entitled "Performance Measurement at Semarang City Samsat 1 using COBIT 5 and the Quality Perception Method". The study was conducted to determine the capability level of service satisfaction in Semarang City Samsat 1. This study aims to help improve service productivity and align the vision and mission of the City of Semarang 1 by optimizing resources. The methodology used is the COBIT 5 framework for measuring capability levels, which focuses on the DSS02, DSS03, and EDM04 processes. Measurement results of the capability level achieved indicate that the capability level of the DSS02 and DSS02 processes = 4.00 (predictable); the EDM04 process = 3.00 (established). And the level of customer satisfaction = 3.91 (satisfied) with the satisfaction indicator is disconfirmation.

2.2. Information Technology Governance Audit Using the Cobit 5 Framework (Case Study: Central Lampung Sea Aquaculture Fisheries) by Suryono [3]
In the journal Management of Information Technology Audit Using the Cobit 5 Framework (Case Study: Lampung Maritime Aquaculture Center) it can be seen that the Lampung Maritime Cultivation Center has used the e-SKP (electronic Employee Performance Target) system. At present information security governance activities have not been carried out to the full. To anticipate the occurrence of obstacles such as human resources who do not understand the e-SKP application so that the potential for errors in the application, then the information technology management method is implemented using the COBIT framework. The processes used in this study are EDM03, APO13, APO12, BAI06, DSS01, DSS02, DSS03, DSS05, MEA01, MEA02. Data analysis uses Maturity Level and Gap Analysis to determine the level of maturity.

2.3. Security Audit on Loan Debit Network Corporation System Using Cobit 5 and ISO 27001: 2013 by Fathoni [4]
Stakeholders in a company have right knowing about optimizing information security management. It can affect a company’s performances and reputation. Information is the biggest business driver in an organization or company. This research aims to measure the capability of the company which is implemented information security governance that impacts on enterprise risk. The Loan Debit Network Corporation System is the main system that supports the company’s business process for corporate lending transactions management. The capability level measurement is based on COBIT 5.0 for Information Security and ISO 27001: 2013 guidelines as a value against the Information Security Governance Component Rating. It starts with aligning organizational goals from COBIT 5.0
perspectives to obtain five COBIT 5.0 IT processes. The Current capability is at level 2.5. Improvement recommendation from level 2.8 to level 3 refers to best practice recommended by COBIT 5.0 for information Security.

3. COBIT and ISO

3.1. COBIT
COBIT (Control Objectives for Information and Related Technology) is an IT governance framework and a set of devices that support and enable managers to bridge the gap existing between control requirements, technical issues and business risk [5]. COBIT provides clear guidelines for controlling IT management in companies with a measure of maturity at each level, this helps organizations to increase the value to be achieved by the use of IT.

COBIT first appeared in 1996, COBIT version 1 which emphasized on audit, COBIT version 2 in 1998, which emphasized the control phase, COBIT version 3 in 2000 which was management-oriented, COBIT version 4 which was more directed towards IT Governance, and The last released was COBIT version 5 in 2012 which led to governance and management for IT company assets. [5]

Although COBIT is known as best practices in IT governance, in fact COBIT has weaknesses, namely:

1. General
   COBIT has 5 domains and many control objectives in it, but COBIT is not intended for certain types of companies. This is a good thing because COBIT can be used in all types of companies, on the other hand this is also a disadvantage because there are several companies with special characteristics such as SOEs or financial service companies so that additional standards are needed that are more detailed.

2. More often used for audits
   COBIT is very popular to be used for audits, where the audit is usually placed at the end of an activity as a reflection and evaluation of activities that are already running. The complexity of COBIT also causes audits not to be done often, usually held every 6 months or once a year. So it can be concluded that COBIT is rarely used as a daily operational standard

3.2. ISO
ISO published by the International Organization for Standardizations (ISO) and the International Electrotechnical Commission (IEC), Founded on February 23, 1947, ISO sets world industrial and commercial standards. ISO, which is an international non-profit institution, was originally formed to create and introduce international standardization for anything. Standards that we are familiar with include standard types of photographic films, phone card sizes, Bank ATM cards, paper sizes and thickness and others. In setting a standard they invited representatives from 130 countries to sit on the Technical Committee (TC), Sub-Committee (SC) and Working Group (WG).

Although ISO is a non-governmental organization, its ability to set standards that often become law through approval or national standards makes it more influential than most other non-governmental organizations, and in practice ISO becomes a consortium with strong relationships with government parties. ISO participants include one national standard body from each country and large companies. ISO itself is a code of practice for providing a framework as a standard. This means providing a high level, general description of the area that should be considered when starting to implement, implement or maintain an activity in management. ISO now does not cover all areas but is still undergoing careful revisions.

The use of ISO related with public trust, a company that already uses the ISO certification is often included in the promotion and profiles. ISO certified companies indicate policies and procedures that are carried out. An organization that applies ISO will have a tool to measure, manage and
control assets that are important for the operation of their systems. This in turn can lead to customer trust, efficiency and effectiveness.

Even though it is expensive, ISO is a popular standard because the application of ISO in a company is useful for:

1. Improve company’s image
2. Improve the company's environmental performance
3. Increase the efficiency of activities
4. Improve organizational management by implementing planning, implementation, measurement and corrective actions (plan, do, check, act)
5. Improve the arrangement of the provisions of the legislation in terms of environmental management
6. Reducing business risk
7. Increase competitiveness
8. Improve internal communication and good relations with various interested parties
9. Get the trust of consumers / work partners / financiers

4. Result

As previously explained, COBIT is a framework within the scope of IT that is the main reference in IT Governance. COBIT is a tool to support and connect the gap between control equipment, technical issues, and business risk. Simply put, COBIT can explain how we solving the problem of securing company assets, technical issues, and risks that can still be measured in a comprehensive manner. Basically, COBIT is a framework (can be interpreted as a guide) is generic (general, with a broad scope) that provides direction on "how should companies / organizations manage IT" (from infrastructure, the people in it, especially related to responsibilities and roles in IT, to the process of acquisition, development, maintenance and documentation to the security of Information Technology in a corporate environment). However, it should be noted. COBIT just shows how to achieve good IT governance criteria. COBIT does not provide details of the implementation of good IT governance. Details of the implementation of good IT governance are left to the use of COBIT. Compared to COBIT , ISO is a more specific, specific, narrow, and detailed framework. ISO provides direction along with guidance and examples in its implementation. Therefore, implementing ISO tends to be easier than COBIT 5, which has a slightly "abstract" language. For example, ISO 17799 talks about IT Security. ISO 17799 is an international standard that provides instructions and controls for regulating information security (Information Security Management Standard / ISMS). Meanwhile, COBIT 5 does not discuss things as detailed as at ISO 17799. However, this does not mean that the two frameworks (COBIT 5 and ISO) are incompatible. In certain cases, COBIT 5 and ISO have the same function. Nevertheless, COBIT 5 and ISO do not clash with each other, instead complementing each other. This can be seen in the Figure below.
COBIT discusses business and IT functional areas in a company and considers IT related to the interests of internal & external stakeholders. The 5 COBIT principles are based on five key principles for corporate governance and IT management as follows:

**Figure 1. Compatibility in IT Governance Framework**

**Figure 2. COBIT 5 Principles**
In the third principle, Applying a single, COBIT 5 integrated network can be adapted to other standards and frameworks, and allows companies to use standards and other frameworks as the scope of management frameworks for enterprise IT. COBIT 5 for Information Security brings knowledge from previous ISACA versions such as COBIT, BMIS, Risk IT, Val IT with guidance from the ISO / IEC 27000 standard which is the ISF standard for information security and the US National Institute of Standards and Technology (NIST) SP800-53A.

5. Conclusion
COBIT provides parameters for assessing how high and how good IT management is at an organization by presenting enterprise stakeholder value, and good governance and management of information assets and technology is needed, including information security arrangements. One of which is included in the COBIT additional standards is ISO, COBIT and ISO in practice can be used together and complement each other because of the characteristics of both. COBIT is a general framework with broad scope so it is more often used at the strategic level, while ISO is a more specific, specific, narrow and detailed framework so that it can be used at the operational level. The second combination can produce a sustainable framework where ISO which regulates more detailed matters is used in daily operations and guidelines, and COBIT as a global framework that regulates decision making and other things on the strategic side.

References
[1] Fox 2003 Rolling Meadows IL: IT Governance Institute.
[2] Dina A 2016 J.of Information System.
[3] Suryono 2018 Jurnal TEKNOINFO
[4] Fathoni 2019 J. Phys.: Conf. Ser. 1196 012033
[5] ISACA 2019 COBIT