Information Technology Governance Analysis to Reduce Information Security Risks Using Cobit 2019: A Case Study of Manufacturing Companies

Aditia Nugroho[1*], Hari Ginardi[2]
Institut Teknologi Sepuluh Nopember (ITS), Indonesia
Email: anugroho.email@gmail.com[1*], hari@its.ac.id[2]

*Correspondence

ABSTRACT

Keywords: IT governance; COBIT 2019; information security.

PT Krakatau Steel (Persero) Tbk is a company engaged in the manufacturing industry that utilizes digital transformation to improve efficiency, optimize facilities and assist organizations in making business decisions quickly. However, there are new challenges in implementing digital transformation, namely increasing dependence on information technology (IT) and triggering high potential threats to information security. Therefore, good information technology governance is needed in managing information security. The research method is based on the Control Objectives for Information Technologies (COBIT) framework version 2019 as the best guide in managing information technology governance. The research was conducted in several stages, including data collection through observation of policy documents and interviews with employees of the BEICT (Business Enables & Information Communication Technology) Department who are responsible for managing services and maintaining the company's digital assets. Evaluation of the maturity level was carried out on 8 priority objectives consisting of EDM03, EDM05, APO12, APO13, APO14, BAI09, DSS05, and MEA04 based on design factor assessment. The results of the analysis of selected domain activities, the IT governance maturity level was at 2.56 (managed level). Indicates that the organization has managed and implemented information security activities, but some activities do not yet have written policies or procedures. With recommendations in the form of proposed improvements to the aspects of people, processes and technology, it is hoped that it can increase the level of maturity of IT governance in reducing information security risks and supporting digital transformation programs.

Introduction

In the era of Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) which describes the business environment is affected by rapid changes, external uncertainty, the complexity of problems and often unpredictable unclarity (Nugroho, 2024). Digital transformation (DT) is one of the strategies for answering various challenges and business sustainability. Digital transformation is the fundamental process of how organizations utilize information technology (IT) to improve performance, efficiency and innovation. The level of adaptation of a company in the era of disruption is greatly influenced by the level of digital transformation and innovation (Škare & Soriano, 2021).

In the implementation of digital transformation, PT Krakatau Steel Tbk as one of the State-Owned Enterprises (SOEs) companies engaged as the largest and integrated steel producer in Indonesia continues to strive for the development of information technology consistently and sustainably to realize the vision of becoming a competitive, profitable and reliable corporation and realize the company's mission in realizing productive and efficient operational performance in producing products and services quality (Tan, Ambouw, & Kustiwi, 2024). The digitalization that has been carried out brings a lot of business operational benefits, especially added value to customers, but it also raises several new challenges to the technological dimension, namely the increasing dependence on information technology in the operational aspect of services, making organizations vulnerable to cyberattacks and the risk of information security breaches such as viruses and data leaks that cause financial impacts (Shiau, Wang, & Zheng, 2023) The results of a survey conducted on chief audit executives from shared countries and industries in Europe (Aqil & Khalid, 2024) showed that as many as 82% of respondents said that data security risks and cyber vulnerabilities are still the number one threat and will still occur in the next three years. Inequality in the application of information technology and increasing vulnerability to information security threats in the government sector and the business world are some of the world's main risks in the next two to five years, along with many other cyber threats such as ransomware. Information security and IT governance are two important aspects of information management in an organization. The two are closely related and influence each other. Effective governance plays an important role in ensuring information protection and security in an organization or country, information security failures can affect the organization's finances and image (Petroye, Liulov, Lytvynchuk, Paida, & Pakhomov, 2020).

IT governance is the process of managing information effectively to achieve organizational goals (Noorhasanah, Winarno, & Adhipta, 2015). This involves setting policies, procedures, and practices related to information management (Alayida, Aisyah, Deliana, & Diva, 2023). Good IT governance will include policies and procedures related to aspects of information security. On the other hand, effective information security requires good governance to manage risk and ensure compliance with established policies and procedures (Oktarina, 2022). Based on the new regulation of the Ministry of SOEs number PER-2/MBU/03/2023 CHAPTER VII article 208 of the implementation of information technology, it is stated that SOEs are obliged to maintain cyber security by the principles of information security which include confidentiality, integrity and availability as well as identifying threats and vulnerabilities in their information technology assets by preparing a cyber incident countermeasure and recovery plan by referring to best practices (Minister of State-Owned Enterprises, 2023).

Control Objective for Information Technologies (COBIT) is an IT governance framework that provides a series of common processes for information technology management, including aspects of information security (Zuraidah, 2020). The advantage of COBIT lies in the integration of information security governance into broader IT governance, allowing for a comprehensive measurement of governance capabilities to achieve the expected goals (Suwandi & Setiawan, 2021).

Krakatau Steel Tbk's IT services are managed by the Business Enabler Information Communication Technology (BEICT) Department as part of supporting the achievement of the strategic objectives of the organization (Maskur, Adolong, & Mokodongan, 2018). The BEICT department has in-depth knowledge of the technology used in the company, ensures technology needs, evaluates solutions and implements appropriate technologies to achieve the organization's business goals, and protects and ensures the company's compliance with applicable regulations on the security of the company's systems and data so that the service can operate properly. Within one year, there were recorded firewall security events that showed several types of inbound and outbound traffic attacks. From the list of traffic anomalies of firewall perimeter devices, it is illustrated that the threat of cyber-attacks faced is quite many and varies in type, ranging from scanning activities, malware and also web application attacks. In addition, there are still reports of incident tickets related to phishing emails, and web defacing masquerading as partners, business partners or official institutions to some employees who try to obtain personal information. Based on these problems, this study aims to analyze the objectives of the IT governance domain based on the COBIT 2019 framework which is in line with the company's goals, measure the level of capability and maturity of governance and management domain activities so that it can improve information technology governance in the scope of information security.

Research Methods

This study adopts the COBIT 2019 (continual improvement life cycle) roadmap implementation approach method which focuses on the design stages and improvement recommendations in the area of information security, the stages carried out are as follows:

Tahap 1 (What are the drivers)

The first step taken in this study is to identify the problems that are the challenges of the organization. Identification is carried out through business process studies and literature reviews. The literature review aims to be a reference in strengthening theories that are relevant to the research. Meanwhile, business studies are the study of company documents. In addition, at this stage, the COBIT domain will be determined using the COBIT 2019 design toolkit based on interviews with BEICT Department Managers on eleven design factors which include company strategy, company goals, IT risk profile, IT key issues, IT development methods that are currently being carried out.

Tahap 2 (Where are we now)

The second stage is to prepare an assessment sheet based on the selected objectives from the results of the factor design assessment, identify Respondents using RACI (Responsible, Accountable, Consulted, Informed) Charts that are tailored to the organizational structure, collect primary and secondary data using a qualitative approach through interviews and observation of several company documents such as policy documents, standard operating procedures, work instructions. Interviews were conducted with individuals and focus group discussions orally by asking questions about the process and activities of COBIT 2019 to parties who have responsibility for services in the BEICT Department of PT Krakatau Steel related to the conditions of governance implementation in the organization. After the data is collected, the data is processed to facilitate the process of analyzing the current IT governance implementation conditions using a process capability scheme based on the Capability Maturity Model Integration (CMMI). In CMMI, maturity levels are defined in 6 levels as presented in Table 1.

Table 1
CMMI COBIT 2019 Maturity Level

Level	Characteristic
0 – *Incomplete*	The process is not implemented, the outcome is unpredictable and there is no clear structure.
1 – *Initial*	The process is not formally planned, or undocumented, the success of the process depends on the individual, not the organization.
2- *Managed*	The process is implemented and carried out based on planning, even though the procedure is not complete or perfect, the results of the process are documented even though it is still not standardized.
3- *Defined*	The process is well documented, standardized throughout the organization, and consistent in the implementation of the process. There are clear guidelines and methods.
4-*Quantitative*	Process performance data is quantitatively measured and controlled, to ensure the process runs efficiently.
5-*Optimizing*	The organization focuses on continuous improvement, there are systematic activities in improving processes based on feedback and analysis.

In assessing process performance, assessment scales are used, including N, P, L, and F. N (not achieved) on a scale of 0 – 14%, in this category the process has not existed or has not been implemented correctly, there is no evidence that the process objectives have been achieved. The P scale (partially achieved) is 15 – 50%, but the implementation of the process is still inconsistent and only in some parts. The L scale (largely achieved) is 50 – 84%, in the category The process is carried out consistently throughout the organization even though there are several shortcomings. F scale (fully achieved) 85 – 100%, in this category the process is fully implemented and all results are expected to have been achieved.

Tahap 3 (Where do we want to be)

At this stage, a comparison of data obtained from research in the field, especially in the area of information security, with the level of capability expected by the company based on the COBIT 2019 framework, is carried out. Gap analysis is used to find the difference between the level of capability obtained to the target level to be achieved so that the extent of the current IT governance implementation process can be analyzed.

Tahap 4 (What needs to be done)

The results of the gap analysis in the previous stage are used as a basis for the improvement plan. The improvement plan contains recommendations that can be carried out by the organization, especially in the BEICT Krakatau Steel Department to improve IT governance related to information security risks by the expected targets. IT governance recommendations are grouped based on aspects of people, processes and technology that have implications for management.

Results and Discussion

The COBIT 2019 Design Factor is several elements that help in determining the priority domain objectives of IT governance that are in line with the specific needs, goals and conditions of an organization. After assessing the design factor (DF1-10), the values for the 40 core models were obtained, and the following results were obtained:

Objective model into > 75 (Important)

1. EDM05 Ensuring Risk Optimization (100)
2. APO12 Risk Management (100)
3. APO14 Data Management (100)
4. BAI09 Asset Management (100)
5. 2. Objective core model with a value of < 75)
6. EDM03 Ensuring Risk Optimization (50)
7. APO13 Security Management (50)
8. DSS05 Security Service Management (50)
9. MEA04 Audit/Asssurance Management (50)

After being communicated with the stakeholders of the BEICT Department, namely the BEICT Department Manager, the objective with a value of 50 will be included in the IT governance review because it is related to the information security aspect. From the objectives that have been agreed upon, then mapping is carried out based on the COBIT Focus Area: Information Security guideline. Table 2 shows a list of 46 processes with a total of 176 COBIT 2019 activities that are on the evaluation list.

Table 2
Number of Objective Domain Activities

Domain	Jumlah Aktivitas
EDM03 — Ensured Risk Optimization	
EDM03.01 Evaluate risk management	7
EDM03.02 Direct risk management	5
EDM03.03 Monitor risk management.	4

EDM05 — Ensured Stakeholder Engagement	
EDM05.01 Evaluate stakeholder engagement and reporting requirements	3
EDM05.02 Direct stakeholder engagement, communication and reporting	2
EDM05.03 Monitor stakeholder engagement	1
APO12 — Managed Risk (Pengelolaan Risiko)	
APO12.01 Collect data	1
APO12.02 Analyze risk	8
APO12.03 Maintain a risk profile	1
APO12.04 Articulate risk	5
APO12.05 Define a risk management action portfolio	3
APO12.06 Respond to risk	1
APO13 — Managed Security	
APO13.01 Establish and maintain an information security management system (ISMS).	7
APO13.02 Define and manage an information security and privacy risk treatment plan	7
APO13.03 Monitor and review the information security management system (ISMS)	5
APO14 — Managed Data	
APO14.01 Define and communicate the organization’s data management strategy and roles and responsibilities.	4
APO14.02 Define and maintain a consistent business glossary	2
APO14.03 Establish the processes and infrastructure for metadata management	2
APO14.04 Define a data quality strategy	4
APO14.05 Establish data profiling methodologies, processes and tools	1
APO14.06 Ensure a data quality assessment approach	1
APO14.07 Define the data cleansing approach.	1
APO14.08 Manage the life cycle of data assets	3
APO14.09 Support data archiving and retention.	1
APO14.10 Manage data backup and restore arrangements	3
BAI09 — Managed Assets	
BAI09.01 Identify and record current assets	4
BAI09.02 Manage critical assets	4
BAI09.03 Manage the asset life cycle	3
BAI09.04 Optimize asset value	6
BAI09.05 Manage licenses	2
DSS05—Managed Security Services	
DSS05.01 Protect against malicious software	2
DSS05.02 Manage network and connectivity security	9
DSS05.03 Manage endpoint security	10
DSS05.04 Manage user identity and logical access.	8
DSS05.05 Manage physical access to I&T assets.	7
DSS05.06 Manage sensitive documents and output devices.	5
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events	5
MEA04 — Managed Assurance	
MEA04.01 Ensure that assurance providers are independent and qualified	1
MEA04.02 Develop risk-based planning of assurance initiatives	4

MEA04.03 Determine the objectives of the assurance initiative.	1
MEA04.04 Define the scope of the assurance initiative	4
MEA04.05 Define the work program for the assurance initiative	6
MEA04.06 Execute the assurance initiative, focusing on design effectiveness	6
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness	4
MEA04.08 Report and follow up on the assurance initiative	1
MEA04.09 Follow up on recommendations and actions	2
Total Aktivitas	176

Respond

This research was conducted in the BEICT Department of PT Krakatau Steel involving managers and personnel who directly manage IT governance policies, IT asset management and support IT services. Respondents were then grouped based on roles and responsibilities using a RACI chart that was adjusted to the selected objectives of the factor design.

Table 3
RACI Chart Tableau 3 RACI Chart

Objective Domain	**BEICT Manager**	**Sr.Spec ICT Governance**	**SuperIndendent ICT Operation & Support**	**Sp.End User Devices & Network**	**Sr.Sp IT System Administration**	**Sr.Analytical Application**
EDM03 — *Ensured Risk Optimization*	C	A	I	I	I	I
EDM05 — *Ensured Stakeholder Engagement*	C	A	I	I	I	I
APO12 — *Managed Risk*	C/I	A	R	R	R	R
APO13 — *Managed Security*	C/I	C/I	A	R	R	R
APO14 — *Managed Data*	C/I	C/I	R	R	R	A
BAI09 — *Managed Assets*	C/I	C/I	R	R	A	R
DSS05—*Managed Security Services*	C/I	C/I	A	R	R	R

MEA04 — *Managed Assurance*	C/I	A	R	R	R	R

After calculating the capacity of each IT governance process, the average value for each domain is obtained. Furthermore, it will be compared with the expected maturity target value. Table 4 describes the results of the gap analysis between the expected maturity level and the current applied to the selected domains.

Table 4
Maturity Level Gap

Objective Domain	Maturity Level	Target Maturity	Gap
EDM03 — Ensured Risk Optimization	2,73	3,00	0,27
EDM05 — Ensured Stakeholder Engagement	2,22	3,00	0,78
APO12 — Managed Risk	2,97	3,00	0,03
APO13 — Managed Security	2,84	3,00	0,16
APO14 — Managed Data	2,28	3,00	0,73
BAI09 — Managed Assets	2,48	3,00	0,52
DSS05—Managed Security Services	2,87	3,00	0,13
MEA04 — Managed Assurance	2,06	3,00	0,94
Cumulative Maturity Level	2.56		

In the capability assessment process, several findings were identified in each domain that were not by the practicality of the COBIT 2019 framework. Table 5 presents an explanation of the findings from each domain.

Table 5
Results of the Evaluation of the Objective Domain Process

IT Process / Sub Domain	Findings
EDM03 — Ensured Risk Optimization	1. There are no competency criteria and special abilities for personnel responsible for managing IT risks. 2. There is no guidance in the form of work instructions for monitoring the effectiveness of the governance process and continuous improvement in risk management.
EDM05 — Ensured Stakeholder Engagement	1. Organizations have not developed clear guidelines in the form of information security reporting policies (explaining the procedures that reporters must follow in reporting incidents, who reports should be filed with, how to report and reporting time limits). 2. There are no guidelines for the preparation of information security status reports, data and information to be collected, analyzed and evaluated for the compiler of the report, the parties who receive the report, the frequency of submission of the report, the format and structure of the report, how the information will be presented, the type of graphs and tables used.

	3. There are no specific guidelines related to filling in performance standard indicators, evaluation and assessment of information security.
APO12 — Managed Risk	1. Organizations have not created policies that define information security gap monitoring. a. Organizations need to develop policies in the form of third-party assessment evaluation guidelines (establishing procedures for evaluation of the results of information security assessments according to the needs and standards of information security), and compile clear guidelines in the form of information security reporting policies (explaining the procedures that must be followed by reporters in reporting incidents, who reports must be submitted to, how to report and reporting time limits).
APO13 — Managed Security	a. It is necessary to prepare and establish special guidelines that regulate cybersecurity reporting practices, recommendations for improvement of SMKI, and SMKI audit reporting mechanisms.
APO14 — Managed Data	1. The implementation of encryption practices has not been fully implemented in the organization. 2. There are no guidelines or standards to protect metadata. 3. There are no standards for reporting data evaluation, monitoring and data maintenance. (Data evaluation report, evaluation process) also guidelines related to server and network configuration management. 4. There has been no standardization or procedure related to data retention policies, data storage plans, or backup data restoration testing for business operations.
BAI09 — Managed Assets	1. It is necessary to add guidelines for the identification of critical server assets, network devices, identification policies and asset criticality assessments that govern how routine schedules, execution methods, and tools are used, to establish and maintain a detailed inventory of all licensed software installed on the company's assets. 2. There is no policy in place for market and technology monitoring (encouraging information security teams to continuously identify new solutions that may be more cost-effective and effective). 3. There are no specific standards related to asset turnover (duration of device use, capacity analysis and asset utilization). 4. There is no standard for asset changes, asset monitoring and reporting, and a policy of periodic asset review (asset review is carried out on a scheduled and thorough basis).
DSS05—Managed Security Services	1. Companies need to make specific policies related to auditing and monitoring (establishing procedures for conducting periodic audits and monitoring), information security, and the use of digital certificates. 2. There are no security testing and auditing policies, patch and vulnerability management policies, system activity monitoring policies, or filter procedures policies restricting communication on the server (access-list implementation).

		3. There is no training SOP related to physical information security awareness, or information security audit process for physical information security.
MEA04 Managed Assurance	—	1. There is no certification policy and a special training program for internal audit teams related to information security that covers the required qualification framework, skills, knowledge and certifications. 2. no policy specifically discusses monitoring security trends (procedures for monitoring trends and latest developments in the domain of information security such as new attacks, new security technologies, new data privacy policies), security threat analysis policies (regulating how to conduct a routine analysis process against information security threats from outside). 3. There is no specific policy that regulates information security audits (objectives, scope, and procedures for implementing organizational information security audits) and follow-up procedures for audit findings (how long is the duration of completing audit findings). 4. Guidelines for audit reporting formats and audit recommendations, especially information security, have not been prepared and there are no guidelines for making and reporting the results of corrective actions on information security.

The identification of findings is followed by recommendations for improvement and improvement of IT governance processes that have implications for information security. Table 6 is a list of solution recommendations based on the COBIT 2019 framework which is grouped into three aspects of people, process and technology that can be considered by the BEICT department in improving the IT governance process.

Table 6
Recommendations for Improving Objective Domain

Aspects	Activity
Browse	a. Companies need to improve the competencies and special abilities of personnel responsible for managing IT risks. b. Companies need to conduct regular physical information security awareness training.
Process	Organizations may consider the preparation of the following guidelines: a. Specific policies that regulate information security audits (objectives, scope, and procedures for implementing information security audits in companies). b. Specific policies that address monitoring security trends (procedures for monitoring the latest trends and developments in the information security domain such as new attacks, new security technologies, and new data privacy policies), security threat analysis policies (regulating the routine analysis process of information security threats from outside) c. Addition *of work instruction* related to filter policy restriction of communication on the server.

	d. System testing standards in the form of *pentests*, *vulnerability assessments*, methods, scenarios, and implementation mechanisms that include the use of methodologies such as OWASP, PTES, and other industry standards to conduct in-depth and systematic penetration testing. e. Unlicensed software check procedures. f. Capacity planning *and* asset *utilization* analysis procedures g. Asset identification & and criticality assessment policy procedures h. Data consistency/integrity reporting and evaluation policies, data testing, and special policies related to data security concerning personal data protection laws. i. Employee surveys and employee awareness related to personal & and company data protection. j. Guidelines for evaluating third-party assessments in the context of information security. k. Information security guidelines in making project proposals related to information security. l. The guidance is in the form of *work instruction on the* monitoring process of the effectiveness of risk identification, and examination of the implementation of actions, so that continuous improvement in risk management. m. Guidelines for incident reporting and information security status (describe the procedures that reporters must follow in reporting incidents, relevant parties that must be informed in the report, and reporting time limits).
Technology	a. Implement data encryption of end-user devices that contain sensitive data. Examples of implementations can include *Windows BitLocker®, Apple FileVault®, and Linux® dm-crypt*. b. Implement automated tools, such as host-based Data Loss Prevention (DLP) tools to identify all sensitive data stored, processed, or transmitted through corporate assets. c. Implement a notification system that can remind (expire) the validity period of *hardware* and *software licenses*.

Conclusion

The results of the COBIT 2019 design factor assessment are based on the vision, mission, strategy and risks faced by the selected organizations in 8 priority objective domains, namely EDM03, EDM05, APO12, APO13, APO14, BAI09, DSS05 and MEA04. 29 processes have a gap in the current level of capability with the target expected by the organization. The level of maturity of IT governance of the BEICT Department is currently at the level of 2.54 (Managed) and has not reached level 3 (Defined), but in general, the process of IT governance activities at PT Krakatau Steel has been carried out, the functioning and responsibilities of the existing organizational structure, and there is support from management, but there is still a need to make some improvements in its implementation, especially in terms of policy preparation, procedures related to the implementation of IT governance activities.

Bibliography

Alayida, Nur Fitria, Aisyah, Tsabita, Deliana, Rahma, & Diva, Kirana. (2023). Pengaruh Digitalisasi Di Era 4.0 Terhadap Para Tenaga Kerja Di Bidang Logistik. *Jurnal Economina*, *2*(1), 254–268.

Aqil, Muhammad, & Khalid, Amina. (2024). *Management Accounting Practices in Mitigating Operational Risk: Navigating Uncertainty in Pakistan Retail*.

Maskur, Maskur, Adolong, Nixon, & Mokodongan, Rusliy. (2018). Implementasi tata kelola teknologi informasi menggunakan framework COBIT 5 di BPMPTSP Bone bolango. *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 109–126.

Noorhasanah, Noorhasanah, Winarno, Wing Wahyu, & Adhipta, Dani. (2015). Evaluasi Tata Kelola Teknologi Informasi Berbasis Framework COBIT 5. *Semnasteknomedia Online*, *3*(1), 1–2.

Nugroho, Aditia. (2024). *Analisis Tata Kelola Teknologi Informasi Untuk Mengurangi Risiko Keamanan Informasi Menggunakan COBIT 2019: Studi Kasus Perusahaan Manufaktur*. Institut Teknologi Sepuluh Nopember.

Oktarina, Tri. (2022). Tata Kelola Teknologi Informasi dengan COBIT. *Tata Kelola Teknologi Informasi Dengan COBIT*.

Petroye, Olha, Liulov, Oleksii Valentynovych, Lytvynchuk, Iryna, Paida, Yurii, & Pakhomov, Volodymyr Vasylovych. (2020). *Effects of information security and innovations on Country's image: Governance aspect*.

Shiau, Wen Lung, Wang, Xiaoqun, & Zheng, Fei. (2023). What are the trends and core knowledge of information security? A citation and co-citation analysis. *Information & Management*, *60*(3), 103774.

Škare, Marinko, & Soriano, Domingo Riberio. (2021). A dynamic panel study on digitalization and firm's agility: What drives agility in advanced economies 2009–2018. *Technological Forecasting and Social Change*, *163*, 120418.

Suwandi, Kevin, & Setiawan, Johan. (2021). Influence of Information Security Culture on the Information Security Governance Capabilities (Case Study: PT XYZ). *Journal of Multidisciplinary Issues*, *1*, 62–74.

Tan, Angelina Wijaya, Ambouw, Nathalie Elshaday Betrix, & Kustiwi, Irda Agustin. (2024). Digitalisasi Ekonomi SIA: Transformasi Sistem Informasi Akuntansi Dalam Meningkatkan Efisiensi Dan Inovasi Bisnis. *Jurnal Mutiara Ilmu Akuntansi*, *2*(2), 332–341.

Zuraidah, Eva. (2020). Audit tata kelola teknologi informasi menggunakan framework cobit 4.1 (pada studi kasus pt anugerah). *PROSISKO: Jurnal Pengembangan Riset*

Dan Observasi Sistem Komputer, *7*(2), 84–95.