GOVITA
JOURNAL GOVERNANCE IT ADOPTION AND TECHNOLOGY ADVANCE

Volume 1, (1) 2026, p. 62-69

Utilization of ISO 27001 in Information System Security Governance Assessment at PT XYZ

Sayyidah Jasinda Amalia[1], Sandhy Fernandez[2*]
[1,2]Sistem Informasi, Universitas Telkom, Purwokerto, Indonesia

[1]20103143@ittelkom-pwt.ac.id , [2]sandhyf@telkomuniversity.ac.id

Submit: 26-01-2026, Revisi: 29-01-2026, Diterima: 02-02-2026, Publikasi: 11-02-2026

***Abstract*—PT XYZ operates in the provision, distribution, and management of clean water resources for the community, yet it faces challenges in information system security because it has not implemented a structured information security management system and relies solely on daily data backups as a risk mitigation measure. This condition is insufficient to protect information assets from security threats such as cyberattacks, data loss, and operational disruptions that may affect service continuity. This study aims to evaluate information system security governance at PT XYZ and identify gaps between current practices and established standards using the ISO/IEC 27001:2013 framework. The study applies a qualitative research method with data collected through direct observation and interviews with personnel involved in information technology management. The results indicate that most ISO 27001:2013 clauses have been implemented adequately; however, weaknesses remain in risk assessment, documentation, and corrective action processes. This study provides improvement recommendations focusing on strengthening security policies, implementing systematic risk management, and conducting continuous security evaluations to enhance the effectiveness of information system protection and support the sustainable operation of PT XYZ.**

Keywords*: *Clean Water Utility, Information Security, ISO 27001:2013, Risk Management, Security Governance

I. INTRODUCTION

Effective information technology management aims to ensure that information technology management supports and is aligned with the business strategy determined by the institution's leadership. [1]. In line with the times that continue to develop, advances in information technology are now happening very quickly [2]. Technological advances in the industrial revolution 4.0 era have a significant influence on company performance [3]. In today's world, information technology plays a crucial role, especially in automating various operational tasks [4]. This automation facilitates a range of services, enhancing both efficiency and effectiveness within companies. In the digital era, companies used digital systems to support services for users, allowing easy access to information and services [5]. The increasing dependence of organizations on the use of information systems on a routine basis is in line with the threats and risks that arise from the use of these information systems [6]. Without adequate protection through network or information system security, organizations risk losing their information assets [7]. Apart from implementing information security management in accordance with applicable standards and protocols, it is important to evaluate or assess the information security management that has been implemented [8]. However, the use of information technology necessitates robust system security to safeguard important company data and ensure specific security measures align with corporate objectives [9]. The role of information system security is vital in meeting company needs such as data and asset storage [10].

This data is very vulnerable to misuse by irresponsible parties. Therefore, security must be one of the main factors considered in the development of information systems [11]. As a preventive measure against cyber-attacks on educational institutions, it is necessary to carry out an information security analysis of existing systems [12]. The goal of information security is to maintain business continuity and reduce any reduction in business value by

*20103143@ittelkom-pwt.ac.id

GOVITA
JOURNAL GOVERNANCE IT ADOPTION AND TECHNOLOGY ADVANCE
Volume 1, (1) 2026, p. 62-69

limiting the effects of security incidents [13]. To ensure the security level within a company is adequate, a standardized assessment framework is necessary for setting information security management system requirements [14]. One such framework is ISO/IEC 27001:2013, a globally recognized security standard that provides a structured approach to securing organizational information [15]. Implementing this standard involves applying controlled security measures to maintain confidentiality, availability, and integrity of information, primarily through risk management procedures [16]. An information security system is also very important because it protects stored data from various threats, such as hacker attacks, viruses or malware [17]. This helps efficiently manage and mitigate risks by authorized personnel, focuses on providing clean water supply services, which can be accessed online [17].

Despite the benefits of such systems, potential risks like cyber-attacks, including data theft, sabotage, and ransomware, pose significant threats to company operations. An interview with PT XYZ's HR and IT departments revealed a ransomware attack that disrupted several servers, corrupted data, and altered file extensions, hindering employees from uploading photos and documents [18]. This incident highlighted the lack of a comprehensive security management system beyond daily data backups. Consequently, it is crucial to assess system security standards using ISO 27001:2013. Adopting ISO 27001:2013 as the framework for this evaluation is apt, given its international recognition and focus on information security management. This research aims to provide recommendations to enhance the company's IT security management, improve overall company performance, and bolster its reputation.

II. LITERATURE REVIEW

Review of previous studies was conducted to provide a deeper understanding of priority strategies for improving IT governance applicable to support this study. Previous studies used to compile this study are as follows:

Based on the analysis conducted by the audit team, PT Indonesia Game has the lowest rating in Annex 7 among the other Annexes because several key documents were found to be unlabeled and several forms did not comply with the procedures listed in the title, resulting in a lack of synchronization. However, overall, ISO 2001:2013 has been well established because it has a mean value of 94.45% with a level of 5 Optimized [9]. Based on further research, it was concluded that the laboratory clinic had identified 35 risks in business development & Information Technology department that were categorized as moderate with a large number of controlled requirements based on ISO/IEC 27001:2013 [10]. Further research and discussion of the results concluded that the Madiun City Communication and Information Agency were categorized into several levels, namely very low, low, and high. With respective risk values of RPN 16, 30 and 56, and 84 and 96. Based on the mapping of ISO 27001:2013 and ISO 27005: 2013, it was concluded that the SOPs in the Communication and Information Agency were 35% adequate and a number of 1 SOPs needed improvement in the incident assessment section that must be fulfilled in ISO 27001:2013 and ISO 27005:2013, which numbered 22 [11].

III. RESEARCH METHODOLOGY

The research begins with identifying problems at PT XYZ using descriptive analysis methods to explore and provide an in-depth understanding of the research topic.

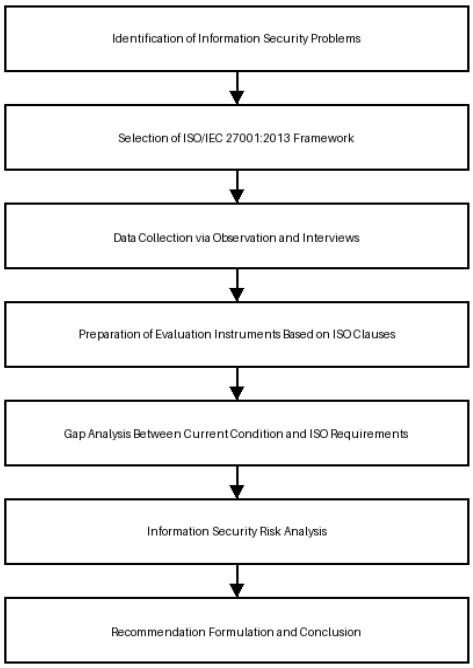

Figure 1. Research Methodology

*20103143@ittelkom-pwt.ac.id

GOVITA
JOURNAL GOVERNANCE IT ADOPTION AND TECHNOLOGY ADVANCE

Volume 1, (1) 2026, p. 62-69

The analysis was conducted based on 10 clauses of the ISO 27001:2013 framework, as follows [19]. Clause 1 – Scope of the Standard: Design, implement and optimize information security management systems, Clause 2 – Normative References: Having norms or regulations that comply with applicable legal guidelines, Clause 3 – Terms and Definitions: Understanding the processes and criteria for information security, Clause 4 – Organizational Context: Determining internal and external issues relevant to organizational goals, Clause 5 – Leadership: Top management having responsibilities and authorities related to information security, Clause 6 – Planning: Risk mitigation and identifying opportunities to achieve information security objectives, Clause 7 – Support: Supporting the sustainability of information security through resources, competence, and communication, Clause 8 – Operation: Planning and controlling operations for effective implementation, Clause 9 – Performance Evaluation: Evaluating the performance of the security system through internal audits, Clause 10 – Improvement: Continuous improvement actions to enhance organizational effectiveness. The analysis of development needs for maximizing data innovation provides comprehensive guidelines to enhance the company's value based on the existing recommendations.

IV. RESULT AND DISCUSSION

Based on the interviews conducted with IT/HR staff at the company, a gap analysis table was created to compare the current state of information security with the requirements of the ISO 27001:2013 standard. There are 10 clauses in ISO/IEC 27001:2013, and for this research, six relevant clauses were selected based on the research scope. These clauses are essential as they align with the objectives of the study. The table 1 summarizes these clauses [20].

Table 1. Clause ISO 27001:2013

Clause	Implementation Process
Clause 4	Organizational Context
Clause 5	Leadership
Clause 6	Planning
Clause 7	Support
Clause 8	Operation
Clause 9	Performance Evaluation
Clause 10	Repair

The next step involved formulating questions for the respondents, whose responses were used for data processing. The questions and corresponding scores are listed in the table 2.

Table 2. Requirement ISO 27001:2013

Number of Clause	Requirement	Score
4	Context of the Organization	
4.1	Gain an in-depth understanding of the organization and its operational context.	
	The organization has a responsible party for clarifying the objectives and goals of information security.	5
	The organization utilizes management team expertise to identify internal factors affecting information security.	5
	The organization considers implementing advanced analytics or information management tools to enhance operational understanding.	5
4.2	Identify and analyze various existing needs.	
	Relevant parties are aware of the importance of the organization's information security management system needs.	5
	The organization can identify and understand the needs of stakeholders related to information security.	5
4.3	The scope of the Information Security Management System is determined	
	The organization can determine the scope of the ISMS.	5
	The organization has concrete procedures to ensure the ISMS scope covers all relevant activities, processes, and locations.	5

*20103143@ittelkom-pwt.ac.id

GOVITA
JOURNAL GOVERNANCE IT ADOPTION AND TECHNOLOGY ADVANCE

Volume 1, (1) 2026, p. 62-69

Number of Clause	Requirement	Score
4.4	Information Security Management System (ISMS)	
	The organization has an effective ISMS in place.	5
	The organization has systematic mechanisms for monitoring regulatory changes that may impact the ISMS.	2

The interviews revealed gaps in five clauses, highlighting areas were needs improvement. The table 3 presents these gaps.

This company has not yet assessed the level of impact and risk associated with the identified non-conformities, which could lead to a significant risk of operational disruption. This could interfere with services or even cause temporary suspension of operations. The analysis based on ISO 27001:2013 revealed several findings, as presented in Table 4.

Table 3. Gap Analysis

Clause	Requirement	Current Condition	Global Condition	Risk
7.1	Resources	No specific metrics for evaluation	Presence of evaluation metrics	Difficulty identifying issues and opportunities
7.5	Documented Information	No documented procedures	Procedures for documented information	Audit and assessment difficulties, inconsistency in results
8.2	Information Security Risk Assessment	No criteria to assess risk impact and probability	Criteria for risk impact and probability	Vulnerability to security threats, inability to identify priority risks
9.1	Monitoring, Measurement, Analysis, and Evaluation	No periodic effectiveness measurement	Periodic effectiveness measurement	Ineffective control leading to undetected risks
10.1	Non-conformity and Corrective Action	No impact and risk assessment for non-conformities	Impact and risk assessment for non-conformities	Significant operational disruptions

Clause 4.1: Understanding the Organization and its Context. The company uses management expertise to identify internal factors and enhance operational understanding for system security. Clause 4.2: Identify and analyze various existing needs. The company analyzes the information security needs of all stakeholders in line with its business plan. Clause 4.3: Determining the Scope of the ISMS. Scope determination follows access rights guidelines, involving the IT sub-department to identify operations, limit scope, update policies, train employees, and evaluate ISMS effectiveness. Clause 4.4: Information Security Management System. Regular mentoring and maintenance ensure ISMS effectiveness, but there's a lack of mechanisms to monitor regulatory changes.

Table 4. Percentage Clause

Clause	Points	Percentage
5.1	Leadership and Commitment	85
5.2	Policies	100
5.3	Functions, Obligations and Authority in Organizational Structure.	100
	Readiness score	**95**
6.1	Strategic Steps to Manage Risk and Take Advantage of Opportunities.	100
6.2	Information Security Goals and Strategy Planning for Achieving Them.	100
	Overall score	**100**
7.1	Resources	80
7.2	Competence	100

*20103143@ittelkom-pwt.ac.id

JOURNAL GOVERNANCE IT ADOPTION AND TECHNOLOGY ADVANCE

Volume 1, (1) 2026, p. 62-69

Clause	Points	Percentage
7.3	Awareness	100
7.4	Communication	100
7.5	Documented Information	90
	Overall score	**94**
8.1	Operational Planning and Control	90
8.2	Information Security Risk Assessment	60
8.3	Information Security Risk Treatment	100
	Overall Score	**83.3**
9.1	Monitoring, Measurement, Analysis, and Evaluation	90
9.2	Internal Audit	100
9.3	Management Review	100
	Overall Score	96.6
10.1	Non-conformity and Corrective Action	60
10.2	Continual Improvement	100
	Overall Score	**80**

Clause 5.1: Leadership and Commitment, Directors are actively involved in ISMS development and maintenance but lack demonstrated support during security emergencies. Clause 5.2: Policies are developed, approved, and maintained by the IT/HR manager, ensuring understanding and compliance among all members. Clause 5.3: Functions, Obligations and Authority in Organizational Structure, Official IT governance policies outlined in the Good Governance Guideline (GGG) are enforced and monitored.

Clause 6.1: Strategic Steps to Manage Risk and Take Advantage of Opportunities, the company addresses security risks through analysis and network/data security enhancements, with documented plans for addressing information security risks. Clause 6.2: Information Security Goals and Strategy Planning for Achieving Them, Objectives are set based on business needs, with interconnected risk evaluation and objective setting, ensuring measurability and achievability.

Clause 7.1: Resources, Necessary resources are provided based on evaluations, but specific metrics to evaluate resource management effectiveness are lacking. Clause 7.2: Competence, Regular training enhances employee competence in information security, with standards set for recruitment and performance evaluations. Clause 7.3: Awareness, Awareness programs focus on system security and data backup to protect against potential threats. Clause 7.4: Communication, Effective communication ensures all employees understand and adhere to information security policies. Clause 7.5: Documented Information, Access restrictions and encryption protect sensitive information, but documented procedures for information management are lacking.

Clause 8.1: Operational Planning and Control, Operational planning involves IT sub-department, with documented control measures, but lacks procedures to ensure policy compliance during operations. Clause 8.2: Information Security Risk Assessment, Critical information assets are identified, but criteria for assessing risk impact and probability are missing. Clause 8.3: Information Security Risk Treatment, Actions are taken to update processes according to the latest technology in response to changes in security risks.

Clause 9.1: Monitoring, Measurement, Analysis, and Evaluation, the company monitors information security monthly but lacks periodic effectiveness measurements. Regular updates are made based on changing information security needs to ensure continued protection and compliance. Clause 9.2: Internal Audit, an internal audit team meets company criteria, with findings and recommendations documented and reported for continuous improvement. Clause 9.3: Management Review, Monthly reviews with HR/IT managers analyze reports to provide insights and incorporate improvements into future plans.

Clause 10.1: Non-conformity and Corrective Action. Currently, there is no assessment of the impact and risk related to identified non-conformities. Quick and effective corrective actions are taken, but the corrective action process is not documented, which is necessary for ensuring long-term effectiveness and accountability. Clause 10.2: Continual Improvement. PT XYZ measures success and continuous improvement in information management by evaluating business plan achievements. Corrective and preventive actions are implemented through analysis and updates to the ISMS to ensure ongoing improvement and adaptation to new challenges.

*20103143@ittelkom-pwt.ac.id

GOVITA
JOURNAL GOVERNANCE IT ADOPTION AND TECHNOLOGY ADVANCE

Volume 1, (1) 2026, p. 62-69

Table 5. Point Clause

No	Clause	Point
4	Organizational Context	92.5
5	Leadership	95
6	Planning	100
7	Support	94
8	Operational	83.3
9	Performance Evaluation	96
10	Improvement	80

The table 6 summarizes the implementation process for each sub-clause:

Table 6. Point for Sub-Clause

Sub Clause	Implementation Process	Percentage
4.1	Gain an in-depth understanding of the organization and its operational context.	100
4.2	Identify and analyze various existing needs.	100
4.3	Determining the scope of the ISMS	100
4.4	Information Security Management System	70
5.1	Leadership and Commitment	85
5.2	Policies	100
5.3	Functions, Obligations and Authority in Organizational Structure.	100
5.4	Leadership	95
6.1	Strategic Steps to Manage Risk and Take Advantage of Opportunities.	100
6.2	Information Security Goals and Strategy Planning for Achieving Them.	100
7.1	Resources	80
7.2	Competence	100
7.3	Awareness	100
7.4	Communication	100
7.5	Documented Information	90
8.1	Operational Planning and Control	90
8.2	Information Security Risk Assessment	60
8.3	Information Security Risk Treatment	100
9.1	Monitoring, Measurement, Analysis, and Evaluation	90
9.2	Internal Audit	100
9.3	Management Review	100
10.1	Non-conformity and Corrective Action	60
10.2	Continual Improvement	100

The gap analysis revealed five clauses needing improvement, with implementation percentages for each sub-clause provided. The highest percentages (100%) indicate full adherence, while the lowest (60%) highlight areas needing enhancement. Recommendations, Clause 4.4: Establish a department for regulatory monitoring and coordination, subscribe to regulatory update services, use compliance management software, and standardize procedures for regulatory changes. Clause 5.1: Create a real-time information security dashboard, emphasize potential incident impacts, and provide guidance for leaders on responding to incidents. Clause 7.1: Apply relevant metrics for resource management evaluation, gather necessary data accurately, use tools like Microsoft Project and Power BI, and conduct regular evaluations. Clause 8.1: Conduct risk assessments, develop understandable security policies, implement appropriate security controls, and ensure legal compliance. Clause 8.2: Develop a risk assessment framework, group risks by type,

*20103143@ittelkom-pwt.ac.id

GOVITA
JOURNAL GOVERNANCE IT ADOPTION AND TECHNOLOGY ADVANCE

Volume 1, (1) 2026, p. 62-69

establish criteria for risk assessment, and use risk management tools. Clause 10.1: Form a team for evaluating non-conformities, use structured approaches for impact and risk assessment, prioritize high-risk issues, take corrective actions, and conduct regular reviews.

V. CONCLUSION

Based on the data analysis conducted, it can be concluded that PT XYZ has successfully implemented the requirements of each sub-clause of ISO 45001:2018. The implementation percentages for sub-clauses 4.1, 4.2, 4.3, 5.2, 5.3, 6.1, 6.2, 7.2, 7.3, 7.4, 8.3, 9.2, 9.3, and 10.2 are 100%, indicating full compliance with these standards. However, sub-clauses 8.1 and 10.1 have the lowest implementation percentage of 60%, suggesting that some aspects of ISO 45001:2018 requirements have not been fully implemented routinely and some requirements remain unmet.

Based on the analysis of the clauses, several recommendations have been made for PT XYZ Firstly, a dedicated department should be established to handle and monitor regulations related to information security. Secondly, it is advisable for the company to develop an information security dashboard to enable real-time security monitoring. Thirdly, relevant matrices should be utilized based on the context of the information system to evaluate the effectiveness of resource management. Fourthly, clear standards and formats should be established for documentation, including document structure, naming conventions, and storage. Lastly, it is important to classify non-conformities based on the level of risk and potential impact, prioritizing the handling of non-conformities with the highest risk.

The implementation of these recommendations is expected to enhance the effectiveness of information security management at PT XYZ, ensuring better protection of the company's data and assets, and achieving comprehensive compliance with ISO 45001:2018 requirements.

REFERENCE

[1] P. Sundari, "SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)," Ultima InfoSys : Jurnal Ilmu Sistem Informasi, vol. 12, no. 1, p. 35, 2021.

[2] A. Kornelia and D. Irawan, "Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1," 2021.

[3] R. Adawiyyah et al., "Pengaruh Keamanan Informasi dan Perkembangan Teknologi di Era Revolusi 4.0 Terhadap Kinerja Perusahaan (Literature Review Manajemen Kinerja)," vol. 2, no. 1, pp. 2829–4599, doi: 10.38035/jim.v2i1.

[4] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)," Jemsi, vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.

[5] H. Sama et al., "Studi Komparasi Framework Nist Dan Iso 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka," Rabit : Jurnal Teknologi dan Sistem Informasi Univrab, vol. 6, no. 2, pp. 116–121, Jul. 2021, doi: 10.36341/rabit.v6i2.1752.

[6] I. Setiawan, A. R. Sekarini, R. Waluyo, and F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 20, no. 2, pp. 389–396, May 2021, doi: 10.30812/matrik.v20i2.1093.

[7] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, "Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi," Jurnal Teknologi Dan Sistem Informasi Bisnis, vol. 6, no. 1, pp. 162–167, Jan. 2024, doi: 10.47233/jteksis.v6i1.1124.

[8] B. Agustami dan B. Syamsul, "Ancaman, Serangan, dan Tindakan Perlindungan pada Keamanan Jaringan atus Sistem Informasi : Systematic Review"Unistek : Jurnal Pendidikan dan Aplikasi Industri, vol.7, no.2, Agustus 2020

[9] S. T. Yuwono, N. Pratama, V. Afifah, P. Minggu, and J. Selatan, "Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK."

[10] N. Diva Ramadhani, W. Hayuhardhika Nugraha Putra, and A. Dwi Herlambang, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)," 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[11] S. K. M. K. Nofri Yudi Arifin et al., Analisa Perancangan Sistem. Cendikia Mulia Mandir, 2022.

*20103143@ittelkom-pwt.ac.id

GOVITA
JOURNAL GOVERNANCE IT ADOPTION AND TECHNOLOGY ADVANCE

Volume 1, (1) 2026, p. 62-69

[12] N. Uswatun Annisa et al., "7 th Conference On Safety Engineering And It's Application Evaluasi Implementasi ISO 45001:2018 di Perusahaan Jasa Layanan Konstruksi Dengan Metode Gap Analysis," 2023.

[13] I. Mantra, A. A. Rahman, and H. Saragih, "Maturity Framework Analysis ISO 27001: 2013 on Indonesian Higher Education," 2020.[Online].Available:www.sciencepubco.com/index.php/IJET

[14] D. Rosita STAI Syekh Manshur Pandeglang, "Ta'dibiya Analisis Ketersediaan Dan Penggunaan Media Pembelajaran Berbasis Teknologi Di Madrasah Ibtidaiyah Syekh Manshur Pandeglang."[Online].Available:http://mulok.library.um.ac.id/oaipmh/../home.

[15] A. Yoshana, M. F. Putra, and N. S. Ulina, "Gap Analysis Implementasi Iso 14000:2015 Pada Pt. Sas International," Jurnal Teknologi dan Manajemen, vol. 19, no. 2, pp. 71–78, Aug. 2021, doi: 10.52330/jtm.v19i2.32.

[16] D. Erlianti, R. Amelia, D. Afrizal, S. Lancang Kuning Dumai, and S. Tuah Negeri, "Jurnal Ilmiah Ekonomi dan Pajak (EJAK) Pelayanan Air Minum Perumda Air Minum Cabang Duri Water Services Perumda Duri Branch," 2022. [Online]. Available: https://ojs-ejak.id/index.php/

[17] S. Tiara et al., "Analisis Perbandingan Cobit 5 Dan Itil V4 Dalam Implementasi It Governance."

[18] B. Panjaitan, L. Abdurrahman, and R. Mulyana, "Menggunakan Kontrol Annex : Studi Kasus Data Center Pt. Xyz The Development Of Information Security Management System Implementation Based On Iso 27001: 2013 Using Annex Control : In Pt. Xyz Case Study Data Center."

[19] B. Al Faruq, "Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT Services and Security Management System," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 3, pp. 3514–3531, Jun. 2020, doi: 10.30534/ijatcse/2020/157932020.