Inovan Publisher

Orbit: Jurnal Ilmu Multidisplin Nusantara

| ISSN (Online) 3064-5883 |
https://creativecommons.org/licenses/by/4.0/
DOI: 10.63217/orbit.v2i4.293

Evaluation of The Effectiveness of ISO\IEC 27001 Based Information Security Audits in State-Owned Telecommunications Companies (Case Study of PT Telkom Indonesia)

Paras Nurhidayati[1], Achmad Fauzi[2], Nayla Shafiya Paramita[3], Renata Viranisa[4], Syalvina Nurhaura Putri[5]
[1]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, paras2nurhidayati@gmail.com
[2]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, naylashafiya048@gmail.com
[4]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, renataviranisa34@gmail.com
[5]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, Syalvinanurhaurap@gmail.com

Corresponding Author: paras2nurhidayati@gmail.com[1]

Abstract: State-owned enterprises have critical information security in the telecommunications sector given the high intensity of strategic data exchange and the sensitivity of the public services they provide. ISO/IEC 27001 has become an international standard that can be widely adopted to ensure systematic, measurable, and sustainable information security management. The telecommunications sector faces many information security risks due to its high dependence on digital infrastructure, the volume of sensitive data, and the increasing intensity of cyber threats. These conditions require us to implement strong security governance through audits based on the international standard ISO/IEC 27001. This study aims to evaluate the effectiveness of information security audits using the ISO/IEC 27001 framework in the telecommunications sector. This study uses a qualitative descriptive method based on audit documents and assessments based on Annex A of ISO/IEC 27001. The results show recurring audit patterns from year to year, weaknesses in several key controls, and irregularities in the follow-up improvement process.

Keywords: ISO/IEC 27001, Security Audit, Information, State-Owned Telecommunications Companies, Audit Effectiveness, Annex A.

INTRODUCTION

The telecommunications sector is one of the industries with the highest level of information security risk due to its high level of dependence on digital infrastructure, the breadth of its services, and the large volume of sensitive data it manages. SOEs in the telecommunications sector have a strategic role as national communication service providers, so that the management of critical assets such as telecommunications networks, operational systems, and customer data becomes a very sensitive issue in relation to cyber threats. The

increasing frequency of cyber intrusion attacks, data theft, ransomware, and access abuse requires the implementation of strong information security practices.

ISO/IEC 27001 is used as a standard that provides a framework for security management systems covering risk management processes, technical controls, and continuous evaluation of information security. Previous studies have shown that the adoption of ISO/IEC 27001 can strengthen information security governance, but the level of effectiveness of its implementation is greatly influenced by the consistency of the audit process and its follow-up. Many organizations still view audits as a formality to meet compliance requirements rather than as a strategic tool to improve security. This has resulted in low audit effectiveness, characterized by recurring findings, lack of follow-up documentation, and weak integration of audit results with continual improvement.

In the case of telecommunications SOEs, the complexity of information makes standards important as a reference for security risk mitigation. This is even more critical because negligence in the audit process can have a significant impact on the security of public services, customer data protection, and the reliability of national infrastructure. Therefore, an evaluation based on the effectiveness of ISO/IEC 27001 audits is important to ensure that audits are not merely administrative activities, but have an impact on the level of information security.

1. To assess the of the implementation of ISO/IEC 27001 audits in state-owned enterprises in the telecommunications sector.
2. To evaluate the of audit effectiveness in supporting the implementation of an information security management system (ISMS).
3. To identify audit findings, causes of recurring findings, and obstacles in audit implementation

METHOD

This study uses a qualitative descriptive research method and literature review conducted by analyzing the data used, namely document analysis with reference to ISO/IEC 27001 Annex A. Annex A contains a list of information security controls that are used as a reference in evaluating the implementation of the Information Security Management System (ISMS). The reason for choosing a qualitative research method was to systematically and objectively describe the conditions of information security implementation in accordance with the ISO/IEC 27001 standard.

This method focuses on a deep understanding of the phenomenon without changing the variables, but rather assessing the data according to the original conditions through observation and interpretation by the researcher. According to Sugiyono (2019), descriptive qualitative research is used to analyze events, phenomena, and social conditions by describing the situation factually and systematically without conducting experiments. This study focuses on: (1) the implementation of ISO/IEC 27001 audits in telecommunications SOEs, (2) the effectiveness of audits in supporting the implementation of information security management systems (ISMS), (3) audit findings, causes of recurring findings, and obstacles in the implementation of audits.

Table 1. Previous Research

No	Name and Tittle	Results of Previous Research	Similarities with This Journal	Differences with This Journal
1	Neaxie, Lidya V, Khairani R. Siregar "Implementation Analysis of Information Security Through Quality Standards ISO 2700 for Internet	The implementation of ISO 27001 is quite good, but internal audits show many findings in Annex A (A.6, A.9, A.10, A.11). There are weaknesses in physical-operational controls and significant network attacks.	Both discuss ISO 27001, the Telkom/BUMN telecommunications study, and use audit findings data.	The main focus is on ISMS implementation and cyber-attacks, not audit effectiveness or recurring findings.

	Services"			
2	Slapničar et al. "Effectiveness of Cybersecurity Audit"	Develops an index for the effectiveness of cybersecurity audits and shows that audit quality does have a significant impact on security maturity within an organization	Supports the analysis of audit effectiveness in this study.	The focus is not on Indonesians or the telecommunications sector.
3	Analysis of Relationships between Non-conformities, Process Maturity and Continual Improvement in Information Security Management Systems"	Found that recurring audit findings are closely related to low process maturity and weak continual improvement.	Reinforces this part of the research regarding recurring findings.	Not specific to the telecommunications sector.
4	Disterer Georg "ISO/IEC 27000, 27001 and 27002 for Information Security Management"	Identifies the ISO 27001 controls that are most often not effectively implemented and explains the challenges for an organization to comply with Annex A.	Analyzing the weaknesses of controls that frequently appear in audits.	The research is more theory-based rather than a case study.
5	Sharma N, Dash P "Effectiveness of ISO 27001 as an Information Security Management: An Analytical Study of Financial Aspects"	Assessing how ISO 27001 can help manage risk and improve information security within an organization.	Both discuss the effectiveness of implementing ISO 27001.	Does not focus on audits or recurring findings.

RESULTS AND DISCUSSION

The Impact of Implementing ISO/IEC 27001 Audits on State-Owned Telecommunications Companies

The implementation of ISO/IEC 27001 audits in telecommunications SOEs certainly has a strategic role, given the high dependence of these organizations on digital infrastructure, network services, and data management on a national scale. One such organization that is highly dependent is Telkom. The complexity of the assets they manage, ranging from their network backbone, data centers, BSS/OSS systems, to services, creates a much greater risk exposure compared to other sectors. In this context, the ISO 27001 audit not only serves as a compliance

t tool, but also as an instrument that is useful for maintaining the stability of public services and national trust. Telkom's position as a major infrastructure provider makes the effectiveness of the audit a determining factor in whether security controls actually work or merely serve as a formality.

In practice, Telkom itself has implemented an ISO 27001 audit cycle, which includes internal audits, surveillance audits, and recertification audits. This mechanism normally involves units such as the Information Security Division, Governance, and internal audit teams that have the role of evaluating the compliance of Annex A controls with actual risk policies. Corrective actions on audit findings are recorded in the GRC system and will be monitored periodically. Although the procedures are quite mature, the patterns of findings that emerge show that many controls are implemented remotely from their operational reality. This is in line with the findings of DNV (2021), which show that controls such as A.9, A.11, and SAN A.12 are often the source of non-compliance in various global organizations.

Audits have a positive impact, as seen in the improvement of internal control formalities, SOP standardization, and a decrease in certain incidents. However, this impact is not entirely optimal due to recurring findings, inconsistencies in controls between units, and a lack of audit integration with IT strategies. An audit culture that typically focuses more on checklists than on the effectiveness of controls results in many audit recommendations that ultimately do not produce significant changes. This is consistent with Serliana & Utamajaya (2025), who assert that audits that are not integrated with risk management tend not to result in significant progress (Serliana Serliana & Joy Nashar Utamajaya, 2025). Thus, the ISO 27001 audit at Telkom is influential, but has not yet achieved its intended effectiveness.

The Influence of Audit Effectiveness in Supporting the Implementation of an Information Security Management System (ISMS)

The effectiveness of ISO/IEC 27001 audits plays a major role in the success of ISMS because audits serve as a validation mechanism for the entire PDCA cycle. When audits are conducted in depth and based on risk, organizations can gain a more accurate understanding of security gaps and the level of compliance with Annex A controls. The audit effectiveness model developed by Slapničar et al. (2022) confirms that quality audits can improve security maturity, and this principle is relevant in the context of Telkom (Slapničar et al., 2022). When auditors not only examine evidence but also evaluate control performance, audits can strengthen ISMS components such as risk assessment, monitoring, and continual improvement.

However, the effectiveness of audits at Telkom is still limited by several factors, such as corrective actions that are often superficial, variability in the capabilities of internal auditors, and the lack of integration of audit results with strategic decision-making, particularly in the allocation of security budgets. This results in audits that should encourage continuous improvement instead only serving as periodic validation. This ineffectiveness can cause several key controls, such as access management and physical security, to remain recurring weaknesses, resulting in suboptimal audit support for ISMS.

Analysis of Audit Findings, Causes of Recurring Audit Findings, and Obstacles in Audit Implementation

ISO/IEC 27001 audit findings at Telkom show a pattern that is consistent with global benchmarks. Controls in domains A.9 (access control), A.11 (physical security), and A.12 (operations security) are the areas with the highest non-compliance, as also found in the DNV global report (2021). These findings include a lack of SOP updates, inconsistent control implementation, documentation that does not reflect changes, and weak verification of compliance activities. This pattern of recurring findings may indicate a gap between system design and day-to-day operations. In terms of risk, non-compliance with these controls can lead to data leaks, illegal access, and disruption of customer services, which ultimately requires strategic attention.

The main cause of recurring findings is weak continual improvement in the ISMS cycle. Naumann (2024) emphasizes that recurring findings generally occur because organizations fail to address the root causes, a pattern that is also seen at Telkom (Naumann et al., 2024). Corrective actions often stop at administrative improvements without any structural and process changes. In addition, inconsistencies in maturity between units lead to the application of different controls, so that audits in subsequent years will find the same problems. Other factors include the limited capacity of internal auditors, the lack of follow-up monitoring after corrective action, and an organizational culture that prioritizes the completion of audits over the effectiveness of controls. The result is that systemic obstacles are not addressed comprehensively.

Audit implementation at Telkom certainly faces various technical, operational, and organizational obstacles. From a technical perspective, Telkom's large-scale infrastructure and involvement of numerous external vendors cause considerable complexity in verifying control effectiveness. From an operational perspective, internal auditors often have limited time and resources, causing them to focus only on documentary evidence rather than assessing operational effectiveness. Culturally, organizations are usually more compliance-driven, so audits are viewed as administrative activities rather than long-term security improvement processes. In addition, audit results are not always based on security strategy planning, so audit recommendations do not have a direct impact on decision-making or security investments. Collectively, these obstacles can hinder the effectiveness of audits in strengthening ISMS.

CONCLUSION

Because the infrastructure data managed by Telkom is highly sensitive, ISO/IEC 27001 plays a very important role for state-owned enterprises in the telecommunications sector. With audits in place, this helps to keep services secure and stable, even though their effectiveness is not yet optimal. Many recurring issues are still found even though audits are carried out regularly, related to physical security and access management and operational security. Controls that are not yet functioning properly in the field are evident from recurring problems. Improvements are also often only administrative in nature, without addressing the root causes of the problems.

Audit results have little impact due to differences in auditor capabilities, an organizational culture that focuses only on fulfilling obligations rather than truly improving security, and the large and complex scale of the system, resulting in audits being treated as a formality rather than an effective tool for improving information security quality. There needs to be consistent follow-up, integration with risk management ( ), and support for increased commitment and capacity in the security culture, so that audits can truly be effective and beneficial. Even so, ISO 27001 audits still provide benefits.

REFERENSI

Boehmer, W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. 2008 Second International Conference on Emerging Security Information, Systems and Technologies, 224–231. https://doi.org/10.1109/SECURWARE.2008.7

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 04(02), 92–100. https://doi.org/10.4236/jis.2013.42011

DNV. (2021). Insights from auditing information security management systems. https://www.dnv.com/article/insights-from-auditing-information-security-management-systems-162216/

Lastyono Putra, E., Cahyo Hidayanto, B., & Maria Astuti, H. (2014). Evaluation of Information Security in the Network of Broadband Division of PT. Telekomunikasi Indonesia Tbk. Using the Information Security Index (KAMI). 3(2).

Naumann, M. M., Olaru, S. M., Lampe, G. S., & Pitz, F. (2024). Analysis of Relationships between Non-conformities, Process Maturity and Continual Improvement in Information Security Management Systems. Proceedings of the International Conference on Business Excellence, 18(1), 494–506. https://doi.org/10.2478/picbe-2024-0043

Neaxie, L. v, & Siregar, K. R. (2014). Implementation Analysis Of Information Security Through Quality Standards ISO 27001 for Internet Services. www.isclo.com

Phirke, A., & Ghorpade-Aher, J. (2019). Best practices of auditing in an organization using ISO 27001 standard. International Journal of Recent Technology and Engineering, 8(2 Special Issue 3), 691–695. https://doi.org/10.35940/ijrte.B1128.0782S319

Prabowo, W. A. (2024). Developing Compliant Audit Information System for Information Security Index: A Study on Enhancing Institutional and Organizational Audits using Web-based Technology and ISO 25010:2011 Total Quality of Use Evaluation. JOIV: International Journal on Informatics Visualization, 8(1), 343.
https://doi.org/10.62527/joiv.8.1.1845

Serliana Serliana, & Joy Nashar Utamajaya. (2025a). Integrated Approach to Information System Auditing: Assessing the Security and Effectiveness of IT Management in the Industry 4.0 Era. JOURNAL OF SCIENCE, TECHNOLOGY AND INFORMATION, 3(2), 7–16. https://doi.org/10.59024/jiti.v3i2.1162

Serliana Serliana, & Joy Nashar Utamajaya. (2025b). An Integrated Approach to Information System Auditing: Assessing the Security and Effectiveness of IT Management in the Industry 4.0 Era. SCIENTIFIC JOURNAL OF SCIENCE, TECHNOLOGY AND INFORMATION, 3(2), 7–16. https://doi.org/10.59024/jiti.v3i2.1162

Sharma, N. K., & Dash, P. K. (2012). EFFECTIVENESS OF ISO 27001, AS AN INFORMATION SECURITY MANAGEMENT SYSTEM: AN ANALYTICAL STUDY OF FINANCIAL ASPECTS. In Far East Journal of Psychology and Business (Vol. 9, Issue 3). www.fareastjournals.com

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. https://doi.org/10.1016/j.accinf.2021.100548

Waluyan, G., & Manuputty, A. D. (2016). Evaluation of IT Governance Performance on the Implementation of the Starclick Framework COBIT 5 Information System (Case Study: PT. Telekomunikasi Indonesia, Tbk Semarang). National Journal of Technology and Information Systems, 2(3), 157–166. https://doi.org/10.25077/TEKNOSI.v2i3.2016.157-166