ZONAsi Jurnal Sistem Informasi
ZONAsi VOL. 7 NO. 3 Sep 2025
Page: 993 - 1007
ISSN: 2656-7407 (Online)
2656-7393 (Print)

OPTIMALIZATION EFFICIENCY OF PAS 99 INTEGRATED MANAGEMENT SYSTEM IMPLEMENTATION ON A STATE-OWNED ENTERPRISE IN TELECOMMUNICATIONS SECTOR

Muhammad Faisal Rahman[1], Diana Ikasari[2]
[1,2]Gunadarma University
(Management Information System Study Program, Master of Technology and Engineering, Gunadarma University)
Jl. Margonda Raya 100 Depok, Depok City, West Java, Phone. 021 7888 1112
e-mail: **me.mfaisalr@gmail.com** , d_ikasari@staff.gunadarma.ac.id

Abstrak

Good Corporate Governance (GCG), sebagaimana diatur dalam PER-2/MBU/03/2023, diharapkan meningkatkan kinerja perusahaan melalui kerangka tata kelola yang efisien. Penerapan GCG kini menjadi standar penting untuk membangun kepercayaan stakeholders, menjamin akuntabilitas, dan mendorong efisiensi tanpa pengulangan siklus PDCA pada setiap sistem manajemen, sehingga integrasi sistem menjadi strategi utama. Penelitian ini mengevaluasi efisiensi implementasi Sistem Manajemen Terintegrasi berbasis ISO 20000-1:2018, ISO 22301:2019, dan ISO 27001:2013 dengan pendekatan PAS 99 pada anak perusahaan BUMN bidang telekomunikasi. Melalui metode kualitatif dan studi kasus, dilakukan gap assessment serta evaluasi siklus PDCA. Hasilnya menunjukkan pengurangan redundansi, peningkatan efisiensi operasional, dan penguatan kapabilitas perusahaan dalam mempertahankan sertifikasi. Faktor keberhasilan meliputi dukungan manajemen, pemahaman konteks organisasi, dan keselarasan prosedur. Disarankan optimalisasi struktur PAS 99 dan peningkatan kapabilitas SDM untuk keberlanjutan sistem.

Kata kunci: PAS 99, ISO 27001, ISO 20000,-1 ISO 22301, Sistem Manajemen Terintegrasi

Abstract

Good Corporate Governance (GCG), as regulated in PER-2/MBU/03/2023, is designed to enhance organizational performance through an efficient governance framework. The implementation of GCG has become a pivotal role in fostering stakeholder trust, ensuring accountability, and improving operational efficiency by minimizing redundancy, particularly in the repetitive application of the Plan-Do-Check-Act (PDCA) cycle cross individual management systems-making system- thereby necessitating system integration. This study evaluates the efficiency of implementing an Integrated Management System (IMS) based on ISO 20000-1:2018; ISO 22301:2019; and ISO 27001:2013 through the PAS 99 framework in a state-owned telecommunications enterprise subsidiary. Employing a qualitative method and case study approach, the research conducts a gap reductions in redundancy, improvements in operational efficiency, and enhanced organizational capability in maintaining certifications. Key success factors includes top management commitment, understanding of organizational context, and procedural alignment across standards. The study recommends leveraging PAS 99 structure more effectively and strengthening human resource capabilities to ensure the long-term sustainability and continuous improvement of the integrated system.

Keywords: *PAS 99, ISO 20000-1, ISO 22301, ISO 27001, Integrated Management System.*

1. PRELIMINARY

Good Corporate Governance (GCG) is a corporate governance principle aimed at established stakeholder rust through systems that regulate, manage, and supervise business control processes to generate added value. GCG also emphasizes the importance of employee, customer, and community concerns in creating a clean, transparent, and professional working environment [1]. This principle is rooted in the concept of good governance, which underscores transparency and accountability.

The application of GCG is based on the Regulation of the Minister of State-Owned Enterprises (BUMN) Number PER-2/MBU/03/2023, which replaces the previous regulation. It is expected that GCG implementation will enhance company performance and create long-term economic value for stakeholders [2], [3], [4]. GCG has now become a critical standard to foster stakeholder trust, ensure accountability, and drive efficiency in implementing management principles—without repeatedly applying the Plan-Do-Check-Act (PDCA) cycle across each management system. As such, system integration has become a vital step in achieving organizational goals [5], [6].

GCG implementation in corporate operations and management is closely linked to the adoption of ISO standards, which provide structured frameworks for effective management systems [7], [8], [9], [10]. The core objective is to enhance organizational sustainability and long-term success while meeting stakeholder expectations. GCG achieves this through sound governance, whereas ISO standards emphasize efficient and effective management system implementation [11].

Founded in 1947 in Geneva, Switzerland, ISO is a non-governmental organization that develops international standards across various industrial and technological domains. These standards are designed to ensure the quality, safety, efficiency, and interoperability of products and services worldwide, involving experts from member countries—including Indonesia.

ISO 27001 is a critical standard for the telecommunications sector, which forms the foundation of Indonesia's digital transformation, particularly in achieving the "Golden Indonesia 2045" vision [12]. While digitalization increases operational efficiency, it also introduces risks, such as cyberattacks that threaten corporate data. Hence, protecting sensitive information is of paramount importance. ISO 27001 supports both IT service management (ISO 20000-1) [13], [14] and business continuity (ISO 22301) [15], [16], [17] by ensuring the availability of essential services during incidents.

Many organizations have adopted multiple Management System Standards (MSS), such as ISO 9001, ISO 14001, and ISO 27001; however, these systems are often implemented in isolation. Integrating management systems can reduce redundancies and enhance efficiency [18]. PAS 99:2012 was developed to simplify the implementation of multiple management system standards and to incorporate new principles outlined in ISO's Annex SL.

This study examines the implementation of an Integrated Management System (IMS) based on ISO 20000-1, ISO 22301, and ISO 27001 and evaluates its effectiveness in meeting certification requirements within a state-owned telecommunications enterprise subsidiary. The research aims to offer insights into the efficiency of ISO standard implementation and how reducing redundancy can lessen operational burdens.

2. RESEARCH METHODS

This study employs the PAS 99:2012 framework, utilizing the Plan-Do-Check-Act (PDCA) approach as the foundational reference for the Integrated Management System (IMS), comprising ISO/IEC 20000-1:2018, ISO 22301:2019, and ISO 27001:2013. These standards guide the design of policies and procedures for the IT Service Management System (SMS), Business Continuity Management System (BCMS), and Information Security Management System (ISMS). Figure 1 outlines the research flow, beginning with a gap assessment and continuing through the Plan, Do, Check, and Act cycles.

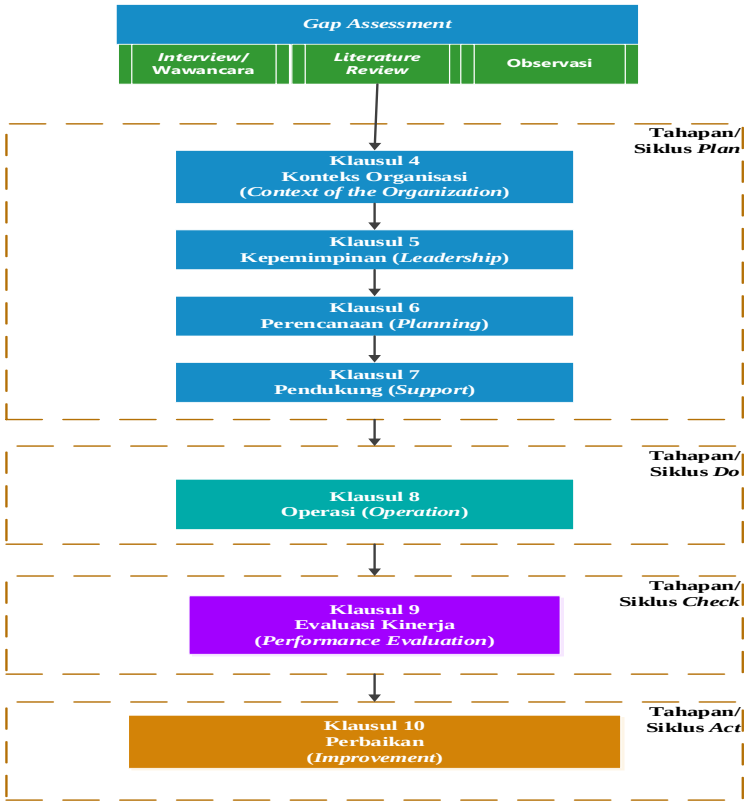

Figure 1 *Flowchart of the Research Stages*

2.1. *Gap Assessment*

The gap assessment phase involves identifying discrepancies between the current state of IT service management and information security at the state-owned telecommunications company's subsidiaries and the requirements set out in ISO 20000-1:2018, ISO 22301:2019, and ISO 27001:2013. At this stage, a review is conducted of the implementation of the Service Management System based on ISO 20000-1:2018, the Business Continuity Management System based on ISO 22301:2019, and the Information Security Management System based on ISO 27001:2013 that has been carried out on the research object by conducting several activities. This phase includes a review of the documents that have been established, interviews with stakeholders, and direct observation at locations included in the scope of implementation and certification activities. The findings are compared with the standards mentioned above. The assessment results are then verified by internal personnel within the organization. If there are any nonconformities or gaps, appropriate corrective recommendations are formulated and integrated into the next PDCA cycle, as shown in Figure 2.

Figure 2 *Gap Assessment Methodology Diagram*

2.2. Plan Phase

The Plan phase focuses on establishing the objectives of the system and its processes, along with the resources required to meet customer requirements and organizational policies. It also involves identifying risks and opportunities. This phase covers Clause 4 (Context of the Organization) through Clause 7 (Support).

2.3. Do Phase

The Do phase is dedicated to the implementation and operation of the management system standards, including the development and execution of policies, procedures, processes, and controls in accordance with Clause 8 (Operation).

2.4. Check Phase

The Check phase involves monitoring and evaluating the processes and planned activities to ensure they are implemented effectively. It is aligned with Clause 9 (Performance Evaluation), which focuses on inspection, analysis, and review of system performance.

2.3. Act Phase

The Act phase is the final step, wherein corrective actions are taken to improve system performance and meet defined requirements. It corresponds to Clause 10 (Improvement) of the management system standards.

3. RESULT AND DISCUSSION

3.1 Gap Assessment

Gap assessment is a method used to identify discrepancies between the current conditions and the ideal implementation of the IT Service Management System (SMS), Business Continuity Management System (BCMS), and Information Security Management System (ISMS). Prior to conducting the gap analysis, the organization collects documents related to the implementation of the integrated management system. These documents include the Integrated Management System Manual, roles and responsibilities of IMS personnel, document control procedures, internal audit policies, and others. During the assessment, conditions were categorized as shown in Table 1.

Table 1 *Condition Status in Gap Assessment Results*

Status	Explanation
Comply	The actual condition fully meets the requirements of the general clauses in the ISO and integrated management system standards.
Partially comply	The actual condition meets only part of the requirements of the general clauses in the ISO and integrated management system standards.
Not comply	The actual condition does not demonstrate conformity with the general clause requirements of ISO and the integrated management system.

The explanation of the condition status in table 1 is the basis for determining the results of the gap assessment of the current condition of the implementation of the Integrated Management System (SMT) implementation based on the ISO 20000-1: 2018, ISO 22301: 2019, and ISO 27001: 2013 standards by BUMN subsidiaries in the Telecommunications sector.

Table 2 *Current IMS Implementation Status against ISO Standard Requirements*

	General Clause of IMS	Specific Clause (ISO 20000-1)	Specific Clause (ISO 22301)	Annex A Controls (ISO 27001)
Comply	**70%**	**48%**	**86%**	**77.14%**
Partially Comply	**30%**	**52%**	**14%**	**22,86%**
Not Comply	**0%**	**0%**	**0%**	**0%**

Table 2 is the result of research related to the existing condition of the integrated management system implementation towards the fulfilment of management system standards that have been implemented in organization (ISO 20000-1, ISO 22301, and ISO 27001).

Based on the findings:

- Out of 20 general IMS clauses, 14 clauses (70%) are fully compliant, and 6 clauses (30%) are only partially compliant, requiring follow-up actions based on provided recommendations.
- For ISO 20000-1:2018 Clause 8 (Operation), 10 out of 21 clauses (48%) are compliant, while 11 clauses (52%) are partially compliant.
- For ISO 22301:2019 Clause 8 (Operation), 6 out of 7 clauses (86%) are compliant, and 1 clause (14%) is partially compliant.
- For ISO 27001:2013 Annex A, 27 out of 35 controls (77.14%) are compliant, and 8 controls (22.86%) are partially compliant.

The identified gaps in the partially compliant clauses across general and specific ISO requirements

The identified gaps in the partially compliant clauses access general and specific ISO requirements are addressed through improvements in the Plan through Act phases.

3.2 Plan Phase

In relation to Clause 4: Context of the Organization, the organization is required to document internal and external factors that influence its operations, identify potential failure risks and their impacts, and define the scope of the IT Service Management System (SMS), Business Continuity Management System (BCMS), and Information Security Management System (ISMS). PT XYZ has documented this in the Management System Context and Scope document. This document outlines internal and external factors that affect the implementation of ISO 20000-1, ISO 22301, and ISO 27001, as summarized in Table 3.

Table 3 *Internal and external factors that can affect the Implementation Management Systems*

Internal Factors	***External Factors***
• *Adding scope and upgrading versions related to the implementation of ISO 20000-1, ISO 22301, ISO 27001 so that it requires changes to documents and implementation;* • *Establishment of One Telin Organizational transformation to support the acceleration of business processes and resource efficiency;* • *The occurrence of the Covid-19 pandemic (New Normal) which has caused a change in the way of working which is currently adopting the way it works with a Hybrid system;* • *Ensuring the feasibility of facilities and infrastructure;* • *Employee competencies that need to be improved in accordance with the requirements of Management System Standards or related regulations;*	• Changes in regulations and changes in force in Indonesia and the country where PT XYZ operates, • Reliability of system management applications provided by third parties; • Insecurity use of devices/systems belonging to third parties related to the risk of interception of information; • Macro economic conditions that have an impact on the weakening of he rupiah exchange rate; • Fulfilling customer expectations to PT XYZ regarding service, business continuity, and information security in PT XYZ; • Competition international businesses that exploit vulnerabilities in the PT XYZ's system; • The development of technologies that encourage the growth of a new product or business in PT XYZ; • Conditions outside the normal that are in the organization such as: power supply failures, fires, demonstrations, wars, floods, and earthquakes; • The development of global issues related to the security of countries in conflict which has given rise to hacker attacks targeting public and private sector business entities; • Threats of cyber attacks such as malware, DDoS attacks, phishing, insider attacks, and software vulnerabilities, include the involvement of

Internal Factors	*External Factors*
	sufficient human and technological resources, rapid changes in policies/procedures, systems with third parties, and the need for rapid response to new and complex issues to ever-evolving technology; • Fulfilment of documents by suppliers, vendors, and contractors related to the Management Systems; • A company environment that is easily provoked to demonstrate; • Policy to obtain permits; • Telecommunication industries policy;

The same document (Management System Context and Scope) also identifies relevant stakeholders and their expectations regarding management system implementation at PT XYZ, as shown in Table 4.

Table 4 *Needs and Expectations from Internal and External Parties related to the Management System*

Internal/External Parties	*Needs/Expectations*
Top Management	**Needs:** The implementation of Service, Information Security, Business Continuity and Occupational Safety and Health Management System in accordance with the requirements of standards, established SLAs, and free from data *loss*/*data leakage*, *illegal access* and losses to the company. **Expectations:** 1) Minimize risks to the company's information assets and services; 2) Implementation of management system policies and objectives that are in line with business needs, the principles of Good Corporate Governance, and applicable laws and regulations 3) Obtain the services needed in accordance with the SLA
Regulator	**Needs:** Compliance with rules and regulations related to the Management System **Expectations:** No violation of established laws and regulations.
Suppliers, Vendors, Contractors, Customers and Partners	**Need:** **The availability of systems or services during the procurement process, and the health and** safety guarantees when carrying out work in TELIN. **Expectations:** 1) Fulfilment of duties and responsibilities of both parties as stipulated in the employment agreement or contract; 2) Availability guidance when doing work in PT XYZ, 3) Zero accident; 4) Uninterrupted services.

Regarding Clause 5: Leadership, as evidence of top management's commitment, PT XYZ has documented the Integrated Management System Manual One Telin, effective September 7, 2023. This manual outlines the delegation of responsibilities and authority to various functions and roles managing the integrated management system. The organizational structure governing the system

is outlined in the Main Duties and Responsibilities of Functional Management System document for ISO 22301:2019, ISO 20000-1:2018, ISO 27001:2013, and ISO 45001:2018.

For Clause 6: Planning, the organization must implement risk-based processes to manage threats to information assets. PT XYZ applies an iterative risk management process including context establishment, risk assessment, treatment, monitoring, review, and communication. These processes are detailed in the Risk Management Policy and Procedures, effective September 7, 2023. Risks—ranging from threats, vulnerabilities, impacts, and opportunities—are recorded in a Risk Register, which includes 120 identified risks, as shown in Table 5.

Table 5 *ISO 20000-1, ISO 22301, and ISO 27001 Management System Risks*

Total of Identified Risk	*120 risks*
Acceptable Risk	116 risks
Risk that need additional control (Risk Treatment Plan)	4 risks

In addition, PT XYZ outlines its system planning efforts in the Management System Objectives and Planning document (effective September 7, 2023), where management objectives are aligned with measurable targets and resource allocation. Details are presented in Table 6.

Table 6 *Management System Goals and Planning*

Objectives	Measurement Metric	Target	Resource Required	Evaluation Method
Awareness personnel	*MS-1*	*All employees who are members of the ISO Team have attended training and programs to increase employee awareness and competence related to the Management System.*	• *Awareness materials* • *Attendance list of participants in the awareness training*	*(Number of employees who have attended the training) / (Number of all employees who are members of the ISO Team) * 100%*
Compliance with IPR	*ISMS-1*	*The number of violations of IPR = 0*	• *Incident Log* • *Information Security Control* • *Internal Audit Results*	*Calculate the number of incidents and audit findings related to IPR*
Management System activity progressed in accordance with the work program which has been set.	*MS-2*	*100% activity of Management System goes according to the work program*	• *Work program* • *Management System Coordinator*	*Evaluation of the realization of Management System activities against work programs*
All the information assets and information processing facilities recorded	*ISMS-2*	*The number of internal audit nonconformities (NC) related asset register*	• *Asset register* • *Internal audit results*	*Evaluation of the list of assets against existing assets*

Objectives	Measurement Metric	Target	Resource Required	Evaluation Method
in the asset register accurately		*are maximum = 10*		*through internal audit*
Risk assessment and review process carried out in accordance with a predetermined schedule	*MS-3*	*Risk assessment is done according to the schedule (at least once a year)*	• *Risk method* • *Risk register*	*Evaluation of the realization of the risk assessment activity schedule in internal audit*
There is no information security incident caused by weakness of physical security	*ISMS-3*	*The number of incidents related to physical security max 1*	• *Incidents report* • *Information security controls*	*Counting the number of information security incidents based on existing incident reports*
There is no information security incident caused by the weakness of the management of access rights	*ISMS-4*	*The number of incidents related to the management of access rights max 1*	• *Incidents report* • *Information security controls*	*Counting the number of information security incidents based on existing incident reports.*
Implementation of testing the continuity of the security of information contained in the Business Continuity Plan	*MS-4*	*The tests carried out at least 1 time/ year according to schedule*	• *Business Continuity Plan* • *BCP Testing Report*	*Evaluation the minutes of the testing*
There is no information security incident caused by ignorance personnel	*ISMS-5*	*The number of incidents related to ignorance personnel max 1*	• *Incidents report* • *Information security controls*	*Counting the number of information security incidents based on existing incident reports.*
Achievement of Service Level (Percentage of overall service achievement)	*SMS-1*	*Min 97%*	• *Measurement and preparation of SLA achievement reports for*	

Objectives	Measurement Metric	Target	Resource Required	Evaluation Method
			each IT Service	
Conformity and accuracy of configuration of each IT Service	*SMS-2*	*50% of all IT Services do not have audit findings related to the completeness and accuracy of their Configuration Items.*	• *Asset Register and Configuration Management Database (CMDB)*	*Number of IT Services for which there are no CI-related findings compared to Number of IT Services.*
IT Service Customer Satisfaction	*SMS-3*	*50% of IT Service customers are satisfied with IT services*	• *Customer Satisfaction Data (Net Promoter Score Summary) IT Services*	*The number of customers who stated satisfaction compared to the number of customers who filled out the complete/valid questionnaire.*
Service Request Management	*SMS-4*	*90% of IT service request reports have been followed up according to the Service Catalog and procedures.*	• *Service Management Procedures* • *IT Service Request Report.*	*The number of IT service request reports that have been followed up is proportional to the number of incoming IT service request reports.*

Finally, for Clause 7: Support, the organization ensures the availability of competent human resources, technology, information, and budgets necessary to develop, operate, and continuously improve the Integrated Management System. Competency and communication guidelines are established in the Awareness and Communication Policy and Procedure, effective September 7, 2023. Awareness initiatives—such as training for ISO 20000-1:2018, ISO 22301:2019, and ISO 27001:2013—have been implemented for team members, as illustrated in figure 3.

Figure 3 *Certificate of Completion for Participating Awareness ISO*

To ensure documentation control, the company has also published the Document and Record Control Policy and Procedure, which governs the documentation processes to support effective system implementation.

3.3 Do Phase

In accordance with Clause 8: Operation, the organization is required to plan, implement, and control its processes to meet management system requirements, including managing planned changes and assessing the impact of unintended changes. Documented control is considered a best practice in this regard; without such documentation, there is a high risk of deviation from established policies and objectives. To support the implementation of the Integrated Management System (IMS), PT XYZ has documented and authorized a comprehensive set of policies and procedures. These documents are categorized according to their relevance to general IMS requirements and specific ISO standards, as summarized in Table 7.

Table 7 *List of Documented Policies and Procedures for IMS and Specific ISO Requirements*

	Document Name
1	*Integrated Management System Manual One Telin*
2	*Main Duties and Responsibilities of Integrated Management System Functions*
3	*Awareness and Communication Policy and Procedure*
4	*Compliance Policy and Procedure*
5	*Management System Context and Scope*
6	*Document and Record Control Policy and Procedure*
7	*Internal Audit Policy and Procedure*
8	*Management Review Policy and Procedure*
9	*Measurement Policy and Procedure*
10	*Nonconformity and Continual Improvement Policy and Procedure*
11	*Management System Objectives and Planning*
12	*Risk Management Policy and Procedure*
13	*Service Catalogue*
14	*Service Management Plan*
15	*Budgeting and Accounting Policy and Procedure*
16	*Business Relationship Management Policy and Procedure*
17	*Capacity Management Policy and Procedure*
18	*Change Management Policy and Procedure*
19	*Design & Transition of New or Changed Service*
20	*Configuration Management Policy and Procedure*
21	*Incident, Service Request and Problem Management Policy and Procedure*
22	*Release and Deployment Management Policy and Procedure*

23	*Service Availability Management Policy and Procedure*
24	*Service Level Management Policy and Procedure*
25	*Service Reporting Policy and Procedure*
26	*Service Continuity Plan*
27	*Business Impact Analysis Policy and Procedure*
28	*Business Continuity Plan Directorate of Technology*
29	*Business Continuity Plan*
30	*Business Continuity Strategy and Solution*
31	*Business Impact Analysis Sub-Group Customer Service Operation*
32	*Business Impact Analysis Sub-Directorate Digital & Service Performance*
33	*Business Impact Analysis Sub-Directorate Digital & Service Planning & Development*
34	*Business Impact Analysis Sub-Group Digital & Service Readiness*
35	*Business Impact Analysis Sub-Group Digital Connectivity Operation*
36	*Business Impact Analysis Sub-Group Digital Platform Operation*
37	*Business Impact Analysis Sub-Group IT Platform Operation*
38	*Business Impact Analysis Sub-Directorate Partnership and Sourcing*
39	*Information Security Policy*
40	*Human Resource Security Policy and Procedure*
41	*Asset Management and End User Security Policy and Procedure*
42	*Access Control Policy and Procedure*
43	*Physical and Environmental Security Policy and Procedure*
44	*Communication and Network Security Policy and Procedure*
45	*Acquisition, Development and Maintenance Security Policy and Procedure*
46	*Supplier Relationship Security and Services Policy and Procedure*
47	*Statement of Applicability*

From the documentation listed above in the Table 7, 47 documents have been officially approved to support the management system implementation at PT XYZ. These include:

- 12 documents dedicated to general IMS requirements;
- 14 documents specific to ISO 20000-1:2018;
- 12 documents specific to ISO 22301:2019;
- 9 documents aligned with ISO 27001:2013 and Annex A Control.

3.4 Check Phase

Aligned with Clause 9: Performance Evaluation, the organization must establish formal processes for monitoring, measuring, analyzing, and evaluating its management system objectives. At PT XYZ, these activities are documented in the Measurement Policy and Procedure, which took effect on September 7, 2023. The monitoring and measurement process is implemented through a standardized Measurement Form for the period from November 2022 to November 2023.

Based on the previously outlined objectives and planning from the Plan Phase (Clause 6: Planning), it was found that 1 out of 13 performance targets was not achieved, as illustrated in Figure 4.

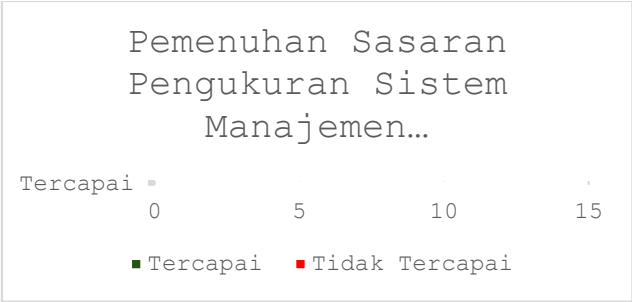

Figure 4 Fulfillment of Integrated Management System Measurement Objectives

The illustration confirms that although most performance indicators were met, continuous evaluation is necessary to ensure full compliance.

PT XYZ also documented its internal audit activities in the Internal Audit Policy and Procedure, effective September 7, 2023. The internal audit was conducted based on the Audit Plan for the Integrated Management System (ISO 20000-1:2018, ISO 22301:2019, and ISO 27001:2013) between September 11 and September 27, 2023. A summary of internal audit findings is presented in Table 8.

***Table 8** Summary of Internal Audit Findings for IMS Implementation*

YEAR	*CERTIFICATIONS*	*MAJOR FINDINGS*	*MINOR FINDINGS*	*OFI (OPPORTUNITY FOR IMPROVEMENT)*
2023	ISO 20000-1:2018	0	3	1
	ISO 22301:2019	0	2	1
	ISO 27001:2013	0	16	12

In addition, PT XYZ management conducts an annual Management Review to ensure continued relevance, adequacy, and effectiveness of the IMS. This activity is governed by the Management Review Policy and Procedure, effective September 7, 2023. The most recent management review meeting was held in a hybrid format on October 2, 2023. The meeting addressed the following key areas:

- Certification scopes for each standard;
- Review of previous management review outcomes;
- Updates on internal and external issues affecting the management systems;
- Certification audit findings and their resolution status;
- Progress toward management system objectives and performance targets;
- Strategic input and direction from relevant stakeholders for continuous improvement.

3.5 Act Phase

In accordance with Clause 10: Improvement, PT XYZ has established and maintained a documented procedure for recording, analyzing, and addressing nonconformities, as outlined in the Nonconformity and Continual Improvement Policy and Procedure. This procedure ensures the continuous improvement of the management system, encompassing IT service delivery, information security, business continuity, and occupational health and safety.

Implementation of this clause includes the execution of external audits by a credible certification body. These audits are conducted in accordance with a pre-approved audit plan and within the scope defined by the organization's certifications.

The Lead Auditor's recommendations from these external audits are summarized below in figure 5 and figure 6.

Figure 5 *Lead Auditor Recommendation for ISO 20000-1:2018*

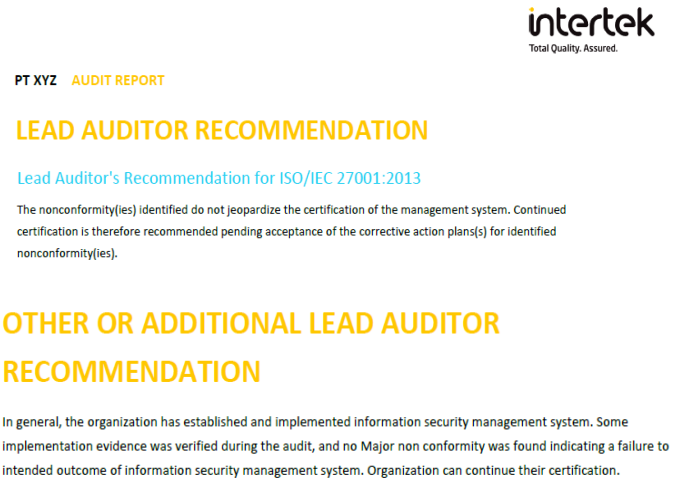

Figure 6 *Lead Auditor Recommendation for ISO 27001:2013*

These recommendations affirm that the organization's integrated management system has demonstrated sufficient compliance and effectiveness to maintain its ISO certifications. However, continuous follow-up and corrective actions on minor findings are necessary to further enhance system performance and ensure alignment with evolving business and regulatory requirements.

3.6 Discussion

The implementation of the Management System in this state-owned telecommunications subsidiary is running well. This is proved by the obtaining and/or successful maintenance of Management System certificates, which indicate that management and implementation are running well and maturely. However, there is still room for improvement to ensure that control implementation is effectively carried out, personnel awareness with the dynamics of rapid personnel turnover and the competencies possessed to be able to implement Management System Standards in the organization. Obviously, this is as well as management's commitment to regulatory compliance and linking this certification to the business processes that have been established in the organization.

4. CONCLUSION

Based on the results and analysis conducted throughout the study, the following conclusions can be drawn:

1) Among the general clause, operational clause, and additional control requirements of the three integrated ISO standard, the majority have met the "Comply" status. However, approximately 30% of general clauses, 52% of ISO 20000-1 clauses, 14% of ISO 22301 clauses, and 23% of ISO 27001 Annex A controls are still in "Partially Comply" status and require enhancements in both documentation and implementation.
2) The most significant gaps were identified in the documentation of system scope, performance measurement, management objectives, execution of internal audits,

management reviews, and the integration of reporting and asset documentation processes. These areas require periodic reviews and alignment across the different standards.

3) The integration of the three ISO standards using the PAS 99 methodology has proven effective in reducing duplication, improving process efficiency, and harmonizing policies, organizational structures, and audit procedures. While unified certification has been successfully achieved, continuous optimization remains essential.
4) Key success factor include: Strong commitment from the top management, readiness and completeness of documentation, personnel competency, IT infrastructure support, and active engagement from all relevant stakeholders. A culture of continuous improvement is crucial to ensuring long-term sustainability and success.

Recommendations for Further Development:

1) Conduct an integrated review and revision of all IMS documentation (scope, audit policies, and performance reports) to ensure consistency across ISO standards and alignment with the PAS 99 framework.
2) Strengthen awareness programs, training sessions, and internal audits regularly to ensure effective implementation and monitoring of all ISO clauses.
3) Periodically update the IT Service Catalog and Information Asset Register in accordance with ISO 20000-1:2018 to maintain data accuracy, capacity management, and optimal system performance.
4) Foster a strong culture of information security, business continuity, and service excellence through targeted training, awareness campaigns, and incentive mechanisms—so that the Integrated Management System becomes an ingrained organizational behavior rather than a mere administrative task.
5) Develop a medium- to long-term implementation roadmap that includes certification scope expansion, digital transformation initiatives, automation of audit processes, and regular evaluations of standard integration—so as to fulfill regulatory requirements and meet evolving customer expectations.

REFERENCES

[1] E. Syofyan, Good Corporate Governance, 2021.
[2] S. D. Luozzo, M. Varisco and M. M. Schiraldi, "The difussion of international standards on managerial practices," *International Journal of Engineering Business Management*, vol. 12, pp. 1-17, 2020.
[3] S. Bakhri and C. Herawati, "KESENJANGAN MANAJEMEN PELAYANAN PUBLIK DI PERBATASANKABUPATEN CIREBON," *Jurnal Manajemen dan Akuntansi*, vol. 14, no. 1, pp. 152-165, 2019.
[4] A. R. Safiih, "PENGARUH MOTIVASI DAN DISIPLIN KERJA TERHADAP KINERJA PEGAWAI PADA PT. KANTOR POS CABANG KEBAYORAN LAMA-JAKARTA," VALUE; *JURNAL MANAJEMEN DAN AKUNTANSI*, vol. 15, no. 2, pp. 107 - 116, 2020.
[5] Y. Suprapto, J. Alvina, K. Khesi and W. William, "Peran Etika, Keberlanjutan, dan Tanggung Jawab Sosial Perusahaan dalam Bisnis International," *SEIKO: Journal of Management & Business*, vol. 6, no. 1, pp. 598-606, 2023.
[6] A. Lopes, D. Polonia, A. Gradim and J. Cunha, "Challenges in the Integration of Quality and Innovation Management Systems," *Standards*, vol. 2, no. 1, pp. 52-65, 2022.
[7] L. M. Tijow and H. Hayat, "Application of Good Corporate Governance (GCG) in State-Owned Enterprises," *ARISTO*, vol. 9, no. 2, pp. 396 - 411, 2021.
[8] I. M. Kom and N. A. I. D. F, "A Bibliometric Analysis of ISO 9000 Research from 2015 to 2020 Using VOSViewer Application," *Library Philosophy and Practice*, pp. 1-10, 2021.
[9] X. Zhao, P. Castka and C. Searcy, "ISO Standards: A Platform for Achieving Sustainable Development Goal 2," *Sustainability*, vol. 12, no. 22, pp. 1-19, 10 November 2020.
[10] M. D. Lisnawita, "Analisis Perbandingan Algoritma Apriori dan Algoritma Eclat dalam Menentukan Pola Peminjaman Buku di Perpustakaan Universitas," *INOVTEK POLBENG - SERI Inform.*, vol. 3, pp. 118–130, 2018.

[11] A. Yunan and E. Nugraha, "INTEGRASI MANAJEMEN KUALITAS SNI DAN ISO DI PERUSAHAAN BADAN USAHA MILIK NEGARA," *JURNAL VALUE: Jurnal Manajemen dan Akuntansi*, vol. 18, no. 3, pp. 951-962, 02 January 2024.
[12] K. Cahyandaru, "Medcom," Medcom.id, 17 December 2024. [Online]. Available: https://www.medcom.id/teknologi/news-teknologi/gNQZeGWb-pemerintah-dan-swasta-harus-bangun-bersama-sektor-telekomunikasi
[13] Benavides-Chicon, C.G., 2020. "Standarization, integration of management systems, cooperative principles and sustainability of tourist companies." *Journal of Tourism and Heritage Research*, 1 April, 3 (2), pp. 29-45.
[14] Tanovic, A & Marjanovic, I. S., 2019. "Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard." *IEEE*, Opatija, Croatia.
[15] Perovic, M. & Todorovic, M. 2024. "INTRODUCING ISO 22301 INTO AN ESTABLISED INTEGRATED." *Technical Faculty "Mihajlo Pupin" Zrenjanin*, pp. 295-301.
[16] Nicolas S, M., & Adrian, G. M., 2024. "Five Standards Model in Information Security Management Systems and Business Continuity." *IEEE*. San Nicolas de los Arroyos, Argentina, pp 1-8.
[17] Aurachman R, Utama, N. I., & Habibie, J. 2021. Information System Control and Improvement Process Design based on Clause 8 ISO 20000-1:2018 using SysML Language. *Purpose-Led Publishing*. Tasikmalaya, Indonesia.
[18] British Standard Institute, "British Standard Institute," 2012. [Online]. Available: https://webstore.ansi.org/preview-pages/BSI/preview_30254209.pdf.