Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Assessing Information Systems and Technology Maturity at the Inspectorate Using IT Balanced Scorecard and ISO 27001

Marice Irianti Mangiwa[1], Benfano Soewito[2*]
Master of Computer Science, Binus University, Jakarta 11530, Indonesia
marice.mangiwa@binus.ac.id[1], bsoewito@binus.edu[2*]
*Corresponding Author: bsoewito@binus.edu

ARTICLE INFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

The development of e-government is currently a significant focus in the public sector, including supervision. As the local supervisory agency, the Regional Inspectorate of Jayawijaya Regency faces challenges in developing Information Systems and Technology (IS/IT) to enhance the Government's Internal Supervisory Apparatus (APIP) capabilities. With numerous supervisory tasks and consulting services, the existing workforce of only 31 employees is insufficient to handle the complex supervisory duties. This study aims to analyze the conditions and challenges the Jayawijaya Regional Inspectorate faces in developing IS/IT. The study uses SWOT analysis, IT Balanced Scorecard, and the implementation of ISO 27001 as key pillars. Through this approach, the internal and external conditions of the organization were explored to formulate appropriate strategies for strengthening the information system. The results of this research include a portfolio comprising information technology business strategies, information systems strategies, IS/IT management strategies, and a roadmap to guide the implementation of sustainable strategic planning for the Jayawijaya Regional Inspectorate.

Keywords: Strategic Planning of Technology and Information Systems,SWOT Analysis, IT Balanced Scorecard, ISO 27001

INTRODUCTION

As stated by the World Bank, good governance is essential for a country's development and prosperity (IMF, 2017). Meanwhile, establishing effective and sustainable governance must align with the rapid growth of information systems and technology, along with strong grassroots movements demanding transparency, accountability, and improved services (Rossieta et al., 2022).The Government of the Republic of Indonesia has acknowledged the importance of implementing principles of good governance to ensure effective, efficient, and accountable public administration (Maranjaya, 2022). This commitment is reflected in various government initiatives and regulatory frameworks aimed at promoting transparency, accountability, and public participation. In this context, information systems and technology (IS/IT) play a crucial role in supporting and enhancing these governance principles (Komite Nasional Kebijakan Governansi, 2022).

Based on Law No. 23 of 2014 on Regional Government, the Regional Inspectorate is responsible for assisting the regional head in guiding and supervising the implementation of government affairs (Puskum dan Humas BPN RI, 2014). The Jayawijaya Regency Government enacts this through Regent Regulation No. 13 of 2021 concerning the Organization and Governance of the Jayawijaya Regency Regional Inspectorate. The Jayawijaya Regional Inspectorate, as part of the Government Internal Supervisory Apparatus (APIP), is responsible for monitoring performance, budget utilization, bureaucratic reform, and regulatory compliance.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Inspectorate carries out its mission to enhance transparency and accountability in regional governance, serving as a quality assurance entity, a consulting partner, and an early warning system. The Inspectorate's role has evolved from a supervisory function to a developmental facilitator across all Regional Apparatus Organizations (OPD) within the Jayawijaya Regency Government (Setyadi, 2021). Currently, the Jayawijaya Inspectorate faces significant challenges, particularly in terms of human resource quantity and competency. With a need for 87 personnel but only 31 available, there is a shortage of 56 staff members. Other issues include inadequate facilities and infrastructure, as well as largely manual applications and systems, leading to delays and risks of errors in reporting.

Given these issues and to support the realization of the Inspectorate's vision and mission, it is essential to develop a Strategic Information System and Information Technology (IS/IT) Plan for the Jayawijaya Regional Inspectorate. This study aims to assess the current situation, and identify weaknesses and deficiencies in the Jayawijaya Regional Inspectorate in relation to IS/IT development. By understanding these conditions, we can provide recommendations for creating a strategic IS/IT plan to support the future enhancement of the Government's Internal Supervisory Apparatus (APIP) capability maturity level. Additionally, the recommended IS/IT strategic planning is expected to serve as a role model for improving the image and performance of the Jayawijaya Regional Inspectorate, guiding more accurate policy and decision-making, and enabling a more comprehensive, measurable IS/IT strategy to support the Inspectorate's vision and mission.

Therefore, in this paper, we will formulate an IS/IT strategy, reassess the current state of the Jayawijaya Regional Inspectorate, and evaluate the IS/IT development status using the IT Balanced Scorecard, combined with SWOT and ISO 27001 analyses. We conduct a standard and needs analysis for IS/IT to align with strategic objectives, followed by a gap analysis between the current and desired states. Finally, the IS/IT strategic plan proposed in this research will proceed to an implementation phase (optional) but will primarily outline a strategic-level roadmap.

Literature Review

The advancement of information systems and technology in government has created various opportunities for organizations to streamline their business processes. Technology can increasingly ease human tasks. Therefore, information systems and technology must continuously evolve across both business and technology domains.

Edhy Sutanta asserts that an information system is a collection of interconnected subsystems working together to process data by receiving inputs, processing them, and producing outputs in the form of useful information for decision-making (Anjeli et al., 2022). Information systems support the operational, managerial, and strategic activities of an organization by leveraging available resources to achieve both current and future goals. In brief, an information system is a set of integrated components designed to collect, store, and process data to provide information, knowledge, and digital products (Vladimir Zwass, 2024). It comprises interrelated components that work toward achieving desired goals (Deni Wahyudi & Rasid Ridho, 2019); (Selay et al., 2023)

From these expert definitions, it is concluded that an information system is a collection of interconnected elements that interact to facilitate decision-making and create new products, organizing a system within an organization to achieve more effective and efficient goals. The components of an information system include: (1) Hardware; (2) Software; (3) Telecommunications networks; (4) Databases; (5) Human resources; (6) Procedures or processes(Pham et al., 2023). These components are interconnected and collaborate to create an effective and efficient information system.

Information technology is a set of tools that assist individuals in working with information and performing tasks related to information processing(Haag & Keen, 1996). The Oxford Dictionary defines information technology as the study or use of electronic tools for storing, analyzing, and distributing various types of information, including words, numbers, and images. Information technology plays a crucial role in the lives of individuals and organizations (Pham et al., 2023), providing the following benefits: (1) Increased work efficiency; (2) Improved communication; (3) Better decision-making; (4)

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhanced innovation; (5) Increased productivity; (6) Improved collaboration and communication among employees and departments; (7) Enhanced information security. According to Kerzner & Saladis (Kerzner & Saladis, 2009), strategic planning is a management tool used to manage current conditions and project future states, which is essential for aligning information technology with organizational objectives.

Strategic Information Systems and Technology Strategy are employed to support business strategy and decision-making. The primary goals of IS/IT implementation are: automating information management processes, enhancing management efficiency, and improving organizational competitiveness (Ward & Peppard, 2002). An information system strategy approach should be aligned with business needs to ensure that IS/IT investments yield benefits.

The strategic IS/IT planning model includes: input activities—engaging with the internal and external business environment, as well as the internal and external IS/IT environment; the IS/IT strategy planning process—systematic steps for formulating, developing, and implementing an IT strategy; output activities—business IS strategy, IT strategy, and IS/IT management strategy; future applications portfolio—applications to be developed in the future; and current applications portfolio—all applications currently in use (Ward & Peppard, 2002). When conducting IS/IT strategic planning, organizations typically choose an established framework to provide structured guidance throughout the planning process, aligning IS/IT planning with the organization's current state.

Three analyses are commonly employed in this planning: SWOT Analysis, IT Balanced Scorecard, and ISO 27001. SWOT Analysis is an acronym for strengths (S), weaknesses (W), opportunities (O), and threats (T) (Renaldo, 2022). This tool groups internal factors (strengths and weaknesses) and external factors (opportunities and threats) that may influence a system internally and externally (Amega et al., 2024). SWOT Analysis aids organizations, both small and large, in identifying competitive opportunities and enhancing performance. The SWOT framework includes: strengths: Internal initiatives that perform well and provide competitive advantage, such as resources, skills, and strong relationships, weaknesses: Poorly performing internal initiatives that hinder progress, indicating areas needing improvement, opportunities: Favorable external conditions, such as new market segments, improved stakeholder relationships, or regulatory changes, and threats: External factors posing risks; unlike weaknesses, they are beyond the organization’s control.

The SWOT Matrix is a tool for developing strategic business components by integrating internal and external factors. The EFAS and IFAS tables record opportunities and threats (EFAS) as well as strengths and weaknesses (IFAS). The SWOT Matrix yields four strategic types: (1) SO Strategy (Strength-Opportunity): Leveraging internal strengths to capitalize on external opportunities; (2) WO Strategy (Weakness-Opportunity): Utilizing external opportunities to address internal weaknesses. (3) ST Strategy (Strength-Threat): Using internal strengths to counteract external threats. (4) WT Strategy (Weakness-Threat): Minimizing internal weaknesses and avoiding external threats (Freddy Rangkuti, 2006).

The IT Balanced Scorecard (IT BSC) is a strategic tool for evaluating organizational decisions based on diverse performance indicators beyond financial metrics. Introduced by Norton and Kaplan in "The Balanced Scorecard: Measures that Drive Performance" (1992), BSC enables easier strategy communication, structured strategy formulation, alignment of departmental goals, and consistent strategy implementation (Kaplan & Norton, 1996);(Usman et al., 2023)

In 1997, Win Van Grembergen adapted the Balanced Scorecard for use in organizational IT departments, arguing that the IT department acts as an internal service provider and should thus be evaluated accordingly (Grembergen & Saull, 2001). IT BSC comprises four perspectives: a. User Orientation: Evaluating user perceptions of IT; b. Operational Excellence: Describing IT processes used to develop and support applications; c. Future Orientation: Encompassing human resources and technologies needed for IT service delivery; d. Business Contribution: Depicting business value derived from IT investment (Grembergen & Saull, 2001).

One of an organization's most valuable assets is information. Leaders involved in strategic policy-making require precise data as a basis for policy. Information is also critical in sustaining ongoing

Research Article

business processes within an organization. To safeguard data, organizations need to plan and establish a secure environment. ISO 27001 is an international standard for Information Security Management Systems (ISMS), designed to protect sensitive information from risks and threats (Calder & Watkins, 2016). This risk management process must integrate with organizational processes and fully incorporate information security into the design of processes, information systems, and controls (Nicho & Muamaar, 2016)

The ability to anticipate information hazards is grounded in the CIA Triad: confidentiality, integrity, and availability of information. These three principles align with ISO 27001's security standards (Eas Certification team, 2023). Almeida et al used COBIT 5 and ISO 27001 to address challenges in the simultaneous implementation of COBIT 5 and ISO 27001, limitations in Enterprise Governance of IT (EGIT) with separate frameworks, and redundancy in organizational resources. This study involved developing an Enterprise Architecture (EA) metamodel, mapping ISO 27001 and COBIT 5, and integrating ISO/EIC TS 33052 and ISO TS 33072 for field assessment. The result was an integrated mapping between COBIT 5 and ISO 27001 using an ArchiMate-based metamodel, facilitating simultaneous evaluation (Almeida et al., 2018). Prabowo addressed IT infrastructure complexity in educational institutions, the vulnerability of IT components to disruptions, and the need for disaster recovery planning. Using DRP development methods based on NIST SP 800-34 Rev.1, the study produced a DRP document tailored to the institution's conditions to strengthen IT resilience (Prabowo Wahyu & Ramadhani, 2021) .

In other Notable Studies, Gazi, Atan, and Kilic analyzed the need for ongoing performance evaluation in the banking sector, addressing cultural factors, entrepreneurship, and the impact of accounting information system effectiveness. The study employed surveys and SEM analysis, showing positive effects on organizational culture, intrapreneurship, and accounting information systems on BSC application (Gazi et al., 2022). The research titled in "Knowledge Management Strategy for Managing Disaster and the COVID-19 Pandemic in Indonesia" used SWOT analysis and ANP to develop accessible strategies for knowledge management related to COVID-19(Oktari et al., 2023). Based on the journal entitled Balanced Scorecard Based Approach In Modeling A Business Intelligence System (Savić & Huđekr, 2023), focused on effective school management, using a BSC-based model to support universal application and user flexibility. And the last, examined security risks in academic information systems, using ISO/IEC 27001 maturity assessment to conclude that information security control is adequately executed at the Faculty of Science and Technology at UIN Syarif Hidayatullah Jakarta (Aini et al., 2024)

The Balanced Scorecard (BSC), developed by Kaplan and Norton in 1992, has become an essential framework for strategy execution in organizations. This study proposes an ontology to bridge the gap between strategy management and data within the BSC framework. The Balanced Scorecard Ontology aids in storing, validating, and analyzing strategy-related knowledge, enabling continuous monitoring and improvement of strategy execution. It enhances interoperability, communication, and alignment between BSC and organizational goals, improving decision-making and governance processes, while facilitating better data integration into the BSC framework(Antunes et al., 2024).The study by the Ministry of XYZ focuses on evaluating the maturity of its Information Security Management System (SMKI) following the implementation of ISO 27001:2013. Despite efforts to align with international standards, a gap remains between technical implementation and governance, as identified in a 2022 Cyber Security Maturity assessment. This research uses an **ISO 27001:2013 Compliance Checklist** to assess and improve the governance of information security, aiming to close existing gaps and ensure the protection of sensitive data (Clarissa & Wang, 2023).

These two studies present highly relevant frameworks for integrating data and strategy within the Balanced Scorecard system, offering valuable insights for improving strategy execution. With their comprehensive approach, these studies serve as strong references for my own work. Similar to the methodology used in these studies, my research aims to bridge critical gaps, particularly in the evaluation and governance of Information Technology strategies. The findings and frameworks

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

proposed in these studies significantly inform the direction of my efforts in assessing and improving information systems and technology maturity.

METHODOLOGY

The research process consists of several steps, namely: literature review, data and information collection, analysis of current conditions, formulation of future requirements, testing of the analysis conducted, and formulation of the SI/TI strategy and portfolio for the future. Figure 1 illustrates the research stages and methodology.

The research begins with a literature review, data and information collection, analysis of current conditions, formulation of future requirements, testing of the conducted analysis, and formulation of the SI/TI strategy and portfolio for the future. In the introductory phase, data and information will be collected, including literature and organizational documents, to support strategic planning for SI/TI that aligns with the vision, mission, and objectives of the Jayawijaya Inspectorate. The second phase involves understanding the current conditions through the analysis of internal and external business environment factors that influence the decision-making process, using business strategy analysis. This includes evaluating organizational performance through SWOT analysis to identify strengths, weaknesses, opportunities, and threats. In this phase, meetings will be held with officials from the Jayawijaya Inspectorate to identify and establish the strengths, weaknesses, opportunities, and threats (SWOT) of the Jayawijaya Inspectorate(Freddy Rangkuti, 2006). The formula for calculating IFAS (Internal Factors Analysis Summary) is as follows:

a. Column 1 (Strengths and Weaknesses): List five internal strengths and five internal weaknesses of the organization or project.
b. Column 2 (Factor Weights): Assign a weight to each factor on a scale of 5 (very important) to 1 (not important), with a total weight not exceeding 1.00.
c. Column 3 (Factor Impact Rating): Assign a rating to each factor on a scale from 4 (very strong) to 1 (not strong). Negative factors are rated as 1.
d. Column 4 (Weighted Score): Multiply the weight in Column 2 by the rating in Column 3 to obtain the weighted score for each factor. Sum all the weighted scores in Column 4 to get the total score, which indicates how internal factors influence the organization's strategy.

The formula for calculating EFAS (External Factors Analysis Summary [17] is as follows:

a. Column 1 (Opportunities and Threats): List five external opportunities and five external threats to the organization or project.
b. Column 2 (Factor Weights): Assign a weight to each factor on a scale from 5 (extremely important) to 1 (not important), with a total weight not exceeding 1.00.
c. Column 3 (Factor Impact Rating): Assign a rating to each factor on a scale from 4 (very strong) to 1 (not strong). Negative factors are rated as 1.
d. Column 4 (Weighted Score): Multiply the weight in Column 2 by the rating in Column 3 to obtain the weighted score for each factor. e. Sum all the weighted scores in Column 4 to get the total score, which shows how external factors influence the organization's strategy.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

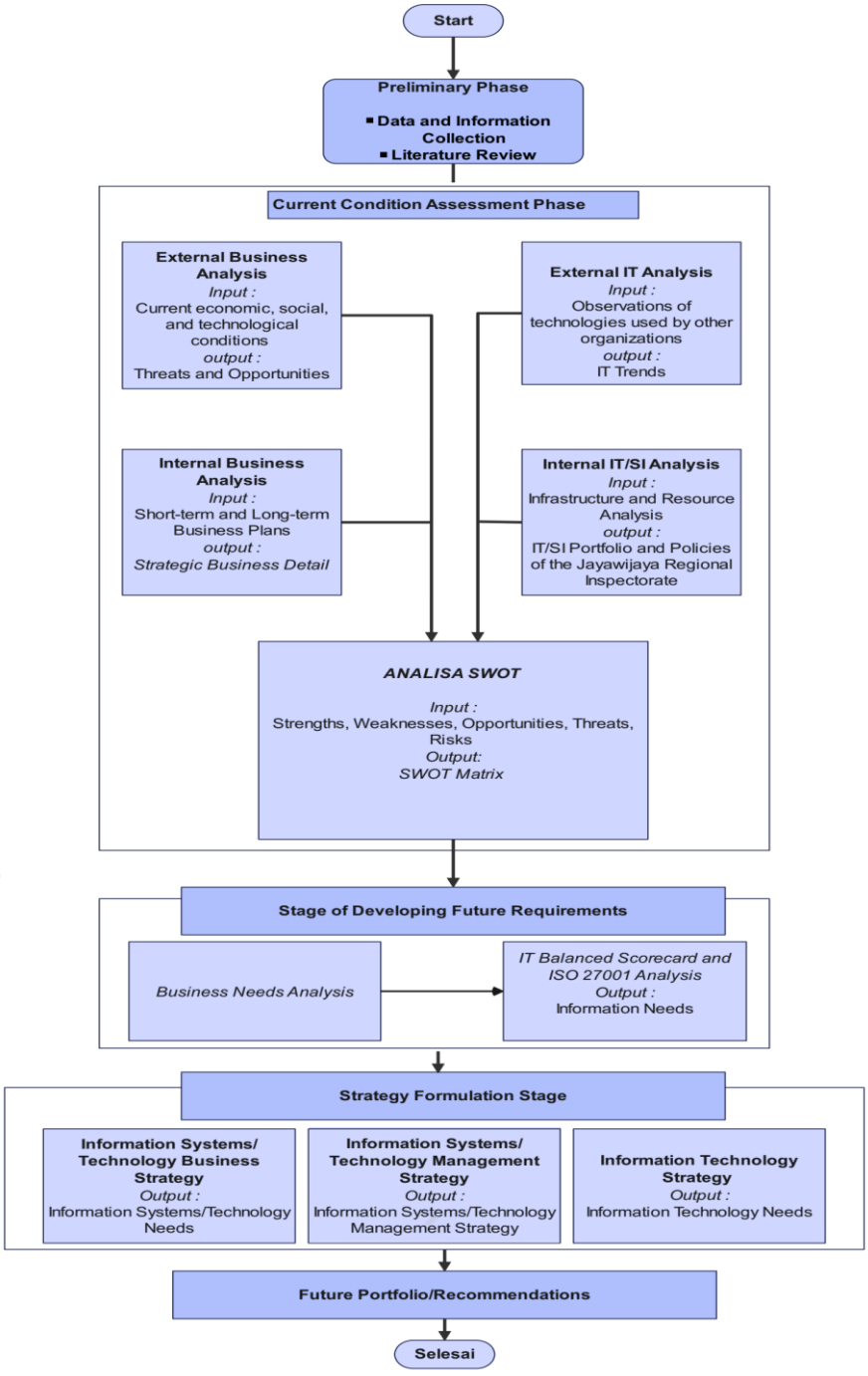

Figure 1 The Research Stage

After obtaining the EFAS and IFAS values, both values will be used to create an equation in order to generate a matrix.

X-axis = Strengths - Weaknesses (1)
Y-axis = Opportunities - Threats (2)

The results of the IFAS and EFAS calculations determine the quadrant position of the Jayawijaya Inspectorate, where the x-axis represents the IFAS calculation results and the y-axis represents the

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

EFAS calculation results. Subsequently, a Strategy Matrix Table is developed using qualitative SWOT analysis, incorporating the factors of strengths, weaknesses, opportunities, and threats into the matrix to derive a combined strategy from these factors.

The third stage focuses on formulating future needs, illustrating the expected conditions based on business and information needs analysis using the Balanced Scorecard. At this stage, a Balanced Scorecard analysis table is also prepared based on the objectives, targets, programs, and activities outlined in the Jayawijaya District Inspectorate's Strategic Plan. The results of this analysis are presented in the form of a map.

To enable the organization to differentiate itself from others, ISO 27001 standards are applied, demonstrating to the public that the organization proactively addresses information threats and uses best practices to mitigate risks. This stage implements the PDCA concept with the use of Annex Clauses, which consist of 14 categories (Putra & Soewito, 2021).

In conducting the maturity level analysis, data from questionnaires will be processed using a formula to calculate the Total Maturity Level (TML) value as follows:

$$\frac{\frac{\Sigma A5}{nA5}+\frac{\Sigma A6}{nA6}+\frac{\Sigma A7}{nA8}+\cdots\frac{\Sigma A18}{nA18}}{n} \quad (3)$$

Explanation:
n = The number of processes in ISO 27001:2013
nA.x = The number of responses obtained from the questionnaire for each clause (Annex) control in ISO 27001:2013

The next, perform a gap analysis to identify the differences between current needs and future needs using the formula:

$$\textit{Gap} = \textit{Expected Score} - \textit{Current Maturity} \quad (4)$$

In the fourth stage, strategy formulation involves developing strategies derived from the previous analysis: Business SI/TI Strategy, SI/TI Management Strategy, and Information Technology Strategy.

The fifth stage integrates the formulated Business SI/TI Strategy and SI/TI Management Strategy into a portfolio, proposing recommendations for the applications needed by the Jayawijaya Inspectorate. The objective of this stage is to determine which applications should be developed based on the analysis results, ensuring that these applications meet the current and future organizational needs, measured using a quadrant approach.

RESULT AND DISCUSSION

The research was conducted at the Regional Inspectorate Office of Jayawijaya Regency, located at the Otonom Weneule Huby Building, Jl. Yos Sudarso, Wamena – Jayawijaya Regency – Papua Mountains Province. In this research, the analysis will focus on understanding the current business conditions, followed by an assessment of future expectations to determine whether they align with the vision and mission of the Inspectorate. Once this is understood, the next step will be to analyze the current state of Information Systems and Information Technology (IS/IT) to ensure that the future development of IS/IT aligns with these expectations. Additionally, the structure and composition of the personnel within the Jayawijaya Inspectorate will be analyzed for suitability

The study began with data collection through interviews, literature review, archival research, and direct observations related to the use of applications, network infrastructure, and business processes within the Regional Inspectorate of Jayawijaya Regency.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Current Condition Assessment Phase

Internal Business Environment Analysis

In the analysis of the internal business environment, interviews were conducted with the Secretary of the Inspectorate, as the position of Inspector is currently held by an acting official. Following this, a process of identifying the institution's general overview was carried out, including its vision, mission, objectives, organizational structure, and the challenges within the scope of the Inspectorate, along with several other analyses. The Regional Inspectorate of Jayawijaya Regency has also outlined these aspects in its Strategic Plan (RENSTRA) for the years 2020-2024. This analysis was conducted to enable the Inspectorate to define its organizational business direction and objectives, as well as identify the factors influencing the Information Systems and Information Technology (IS/IT) needs that could be developed.

The direction and objectives of the Jayawijaya Inspectorate are reflected in the vision and mission of the Jayawijaya Regency. To achieve this vision, specific targets were set, including:

1. Improved quality of performance accountability implementation;
2. Enhanced financial management quality;
3. Increased internal control quality within the Jayawijaya Regency Government;
4. Strengthened capacity of the Inspectorate;
5. Improved quality of financial governance and Inspectorate performance.

In its efforts to implement good governance, the Inspectorate continuously evaluates itself by improving the quality of leadership and staff through training programs and technical guidance. Additionally, the Inspectorate needs to foster innovation to the governance of organizational business continuity, to effectively carry out its responsibilities. The results of the internal business environment analysis conducted at the Jayawijaya District Inspectorate are demonstrated in Table 1.

External Business Environment Analysis

The external business environment analysis of the Jayawijaya Distric Inspectorate reveals several key factors that influence its operations. Politically, instability, social and ethnic conflicts, and corruption are significant challenges that could affect governance and policy-making. Economically, issues such as income inequality, limited local resources, and insufficient infrastructure investment may hinder the Inspectorate's ability to perform effectively. Socially, rising public awareness of accountability, increasing public participation, and the role of media and activists are crucial in strengthening oversight functions. Technologically, the lack of ICT infrastructure, evolving digital platforms, and government policies on technology adoption offer both challenges and opportunities to improve the efficiency and effectiveness of the Inspectorate's operations.

In summary, the Inspectorate must navigate these external factors to optimize its business processes, enhance service delivery, and improve governance through strategic alignment with political, economic, social, and technological trends.

Analysis of Internal IT/IS Environment

The internal analysis of information technology at the Jayawijaya District Inspectorate was carried out by reviewing the current infrastructure, including hardware such as 1 server unit, 18 desktop PCs, 10 laptops, 12 printers, 4 scanners, 2 switches, 2 hubs, and 2 routers. Overall, the number of computers and laptops available is sufficient for business operations. However, due to ongoing technological advancements and increasing workload, the quality of hardware needs to be upgraded. Additionally, some software tools require updates to ensure smooth operations. The internal IT/IS analysis also included an evaluation of the network infrastructure. Currently, the Inspectorate uses internet services from a provider, with servers supplied by the Jayawijaya District Government.

The network topology used by the Inspectorate is illustrated in Figure 2.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1 The Results of the Internal Business Environment Analysis

Code	Analysis Results
LIB 1	There are regulations and policies in the field of supervision that govern the performance of the Inspectorate
LIB 2	Availability of human resources in the supervisory apparatus, although the number of available HR does not yet meet the workload
LIB 3	Availability of sufficient budget
LIB 4	There is motivation to work more optimally
LIB 5	Facilities and equipment are well-maintained
LIB 6	Lack of attention from leadership regarding job description distribution
LIB 7	Lack of specific SOPs for the development of SI/TI
LIB 8	Lack of innovation in the development of integrated SI/TI

Table 2 The Result of the External SI/TI Environment Analysis

Code	Analysis Results
TI-01	Wireless Networks and Mobility
TI-02	Cloud Computing
TI-03	AI-based Network Security
TD-01	Social Media
TD-02	Mobile Computing
TD-03	Data Analytics
TD-04	Cybersecurity
TD-05	Internet of Things (IoT)
TD-06	Blockchain
TD-07	AR and VR
TD-08	Edge Computing:
TD-09	Robotic Process Automation (RPA):
SI-01	Aplikasi Berbasis Web
SI-02	Aplikasi Berbasis Mobile
SI-03	Analitik Kuat pada Aplikasi Web

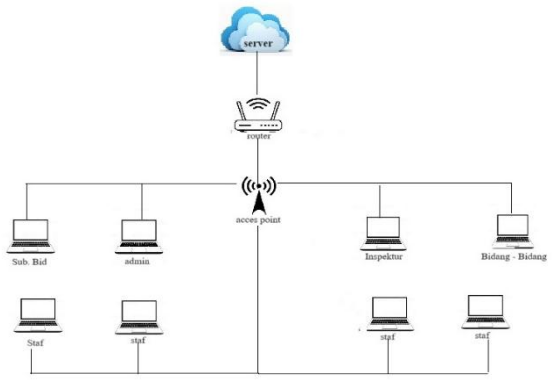

Figure 2. Network Architecture of the Inspektorat of Jayawijaya

This analysis also includes an organizational assessment, which is essential to confirm whether the existing resources within the Inspectorate are sufficient to address issues related to the internal environment of IT/IS. The result of the analysis of the availability and the human resources (HR) requirements at the Inspectorate is displayed in Tabel 3. Currently, the Inspectorate has 31 employees but faces a shortage of 56 staff members. Moreover, based on the current roster, the Inspectorate lacks

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

dedicated IT personnel. As a result, the IT functions are handled by staff from the planning division and outsourced third-party services.

The analysis also highlights the following key Information Systems/Technology (SI/TI) management policies:

1. Provision of Adequate Infrastructure: Ensuring sufficient infrastructure to support supervision and reporting systems.
2. Ensuring Network Security and Reliability: Implementing a secure and reliable computer network, including wireless technologies, cloud systems, and regular data backups to minimize the risk of data loss.
3. Implementing Information and Data Security Measures: Taking steps to safeguard information and data, such as installing firewalls.
4. Developing Staff Competencies in IT Infrastructure: Enhancing the capability of Inspectorate staff to operate and maintain IT infrastructure, through regular training and workshops.
5. Upgrading Hardware and Software: Upgrading hardware and software in line with evolving needs.
6. Supporting IT-Based Innovations: Encouraging innovations based on IT/SI across the staff.
7. Using IT/SI to Enhance Public Access to Performance-Related Information: Utilizing SI/TI to improve public access to information related to performance and oversight activities.

Table 3 Analysis of Human Resource Needs at the Inspectorate

Position Level	Required HR	Available HR	Difference (More/ Less)
Inspector	1	-	1
Secretary	1	1	-
Assistant Inspector	5	5	-
Head of Subdivision	3	3	-
Staff of Subdivision	15	12	3
Senior Auditor	2	-	2
Intermediate Auditor	6	3	3
Junior Auditor	18	5	13
First Auditor	27	2	25
Supervising Auditor	3	-	3
Advanced Implementing Auditor	3	-	3
Implementing Auditor	3	-	3
Total	87	31	56

These policies reflect the Inspectorate's commitment to strengthening its internal capabilities, improving transparency, and ensuring robust governance in the face of technological advancements. In addition, the portfolio of applications currently used by the Jayawijaya Inspectorate has been documented and outlined in Table 4.

Table 4 The portfolio currently implemented by the Inspectorate.

Strategic	***High Potential***
Website	SIPD-RI KapaAPIP SIPTL SITPP LHKPN MCP
Key Potential	***Support***
-	*Google Docs* *Google sheet* *Ms. Word, Excel* *PPT*

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Analisis SWOT

To conduct this SWOT analysis, a questionnaire was distributed to 10 respondents, including the Acting Inspector, the Assistant Inspectors for Regions II, III, and IV, the Heads of Subdivisions as executors, Auditors, and staff as implementers. Tables 5 and 6 show the results of EFAS and IFAS.

This analysis provides insight into the strategic factors impacting the internal and external environments of the Inspectorate, serving as a foundation for formulating relevant strategies to enhance organizational effectiveness. The values/scores derived from each factor of the internal and external environment analysis will represent points.

The values/scores derived from each factor of the internal and external environment analysis will represent points on the following diagram:

X = Strength - Weakness = 3.54 - 1.77 = 1.77
Y = Opportunity - Threat = 2.88 - 2.59 = 0.29

From the calculations above, a matrix is created, as shown in Figure 3.

Table 5 Determination of Weight and Score for Internal Strategic Factors (IFAS)

Code	Internal Strategic Factors (IFAS)	Weight	Rating	Score
1	*2*	*3*	*4*	*5*
	(Strength)			
S1	High usage of IT in job tasks	0,17	3,25	0,55
S2	Availability of facilities and infrastructure	0,17	4,00	0,66
S3	Clear business processes and SOP	0,17	3,75	0,62
S4	Available budget	0,17	3,00	0,50
S5	Leadership commitment to improving the role of supervision	0,17	4,00	0,66
S6	Easy access to information	0,17	3,25	0,55
	Total *Strength*	**1,00**	**21,25**	**3,54**
	(Weakness)			
W1	Limited IT-savvy personnel and lack of a dedicated IT team	0,22	1,67	0,37
W2	Lack of functional oversight competency	0,20	1,08	0,21
W3	Limiited supporting infrastructure, such as an unstable internet connection	0,19	2,00	0,38
W4	Limited data coverage, completeness, and information systems for oversight	0,18	1,83	0,33
W5	Weak public coordination and communication ability	0,21	2,25	0,48
	Total *Weakness*	**1,00**	**8,83**	**1,77**

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 6 Determination of Weight and Score for Eksternal Strategic Factors (IFAS)

Code	Eksternal Strategic Factors (IFAS)	Weight	Rating	Score
1	*2*	*3*	*4*	*5*
	(Opportunities)			
O1	Supportive legislation and government policies	0,17	2,75	0,47
O2	Strong backing from the Regent for the Inspectorate's existence	0,15	3,00	0,46
O3	Limited access capabilities for IT development	0,16	3,42	0,55
O4	Standardization of data content and formats used	0,19	3,00	0,56
O5	High interest and appreciation from stakeholders	0,15	2,83	0,43
O6	High social, economic, and cultural dynamics	0,18	2,33	0,42
	Total *Opportunities*	**1,00**	**17,33**	**2,88**
	(Threats)			
T1	Frequent changes in policies and regulations	0,18	2,58	0,46
T2	Rising public demands for accountability, efficiency, and transparency	0,19	3,00	0,56
T3	Limited access capabilities for IT development	0,16	2,00	0,31
T4	Lack of integration in supervision and evaluation systems	0,16	2,25	0,35
T5	Weak synergy in oversight programs with national and local governments	0,15	2,75	0,40
T6	Rapid technological advancements	0,18	2,83	0,50
	Total *Threats*	**1,00**	**15,42**	**2,59**

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

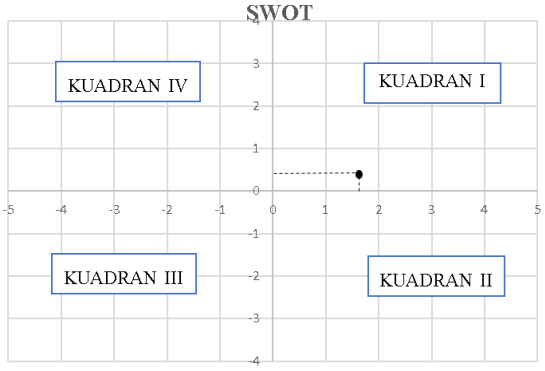

Figure 3 SWOT Matrix

Figure 3 reveals that the current condition of the Jayawijaya Regional Inspectorate is positioned in Quadrant I. This means that the Inspectorate is in a very favorable position, with internal strengths and external opportunities being more dominant. This indicates that the organization is in an advantageous situation. The Inspectorate still possesses significant strengths and can leverage existing external opportunities to address internal weaknesses and avoid external threats. Based on this analysis, strategies have been developed, including Weakness-Opportunity (WO), Strength-Threat (ST), or Weakness-Threat (WT) strategies, to achieve the desired condition.

The Stage of Preparing Future Needs
Business Needs Analysis

In this section, the business processes related to the flow of information and the support of information systems for the business processes occurring at the Jayawijaya Regional Inspectorate are depicted. The business needs analysis at the Jayawijaya Regional Inspectorate for the future is conducted using several analytical models, including:

a. Value Chain Analysis

Value chain analysis is an approach used to understand how an organization creates value for its customers through a series of activities carried out within its business processes. By utilizing the value chain, the Inspectorate can formulate strategies and determine how the information systems to be implemented can support each of these activities. In this context, we will divide the analysis into two parts: primary activities and support activities. Following an observation at the Jayawijaya Regional Inspectorate, the results can be seen in Figure 4.

Table 7 SWOT Strategies for the Jayawijaya Regional Inspectorate

S-O Strategies	***W-O Strategies***
1. Optimize the use of IT systems (S1, S2) by leveraging regulatory and government policy support (O1, O2) to strengthen the Inspectorate's supervisory role. 2. Enhance leadership commitment (S5) to adjust infrastructure according to technological developments and digital media (O3). 3. Utilize clear business processes and SOPs (S3) to respond to high public appreciation and the dynamic role of supervision (O5, O6).	1. Improve the competency of functional officials (W2) through training aligned with the potential for IT advancements (O3). 2. Enhance infrastructure (W3) by utilizing support from the regional government (O2). 3. Address limitations in oversight data (W4) by standardizing data formats (O4).

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Strategi S-T	***Strategi W-T***
1. Use easy access to information (S6) to address policy changes (T1) and meet increasing public demands for transparency (T2). 2. Utilize leadership commitment (S5) to increase program synergy with the Central Government and other regions (T5).	1. Increase IT competency among personnel (W1, W2) to address rapid technological advancements (T6) and challenges in system integration (T3, T4). 2. Develop inter-agency coordination to overcome weak public communication (W5) and program synergy issues (T5).

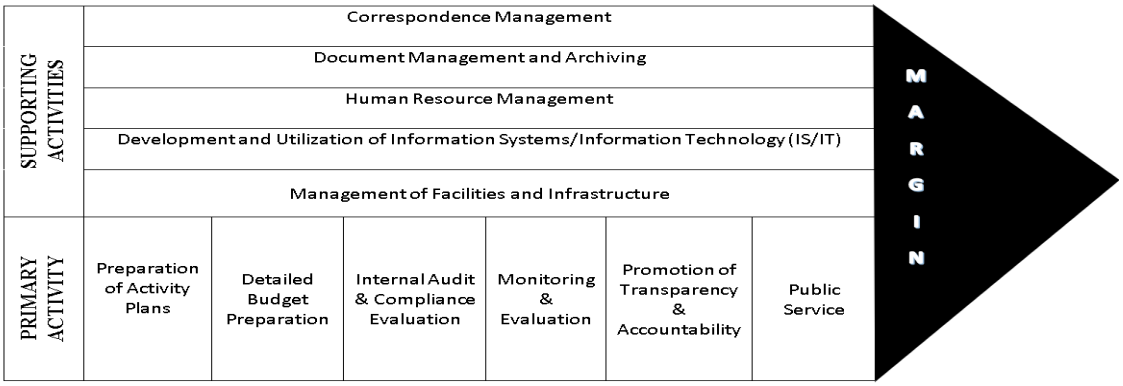

Figure 4 Value Chain

b. IT Balanced Scorecard Analysis

The IT Balanced Scorecard analysis includes four key perspectives: (1) Corporate Contribution, (2) User Orientation, (3) Operational Excellence, and (4) Future Orientation. To effectively implement these perspectives, Key Performance Indicators (KPIs) are essential. The development of KPIs by the Inspectorate of Jayawijaya is critical for enhancing the organization's performance. The Balanced Scorecard is grounded in the Strategic Business Process Plan developed by the Inspectorate of Jayawijaya, which includes initiatives supporting the goals, objectives, vision, and mission. This plan has been aligned with the Jayawijaya's Medium-Term Regional Development Plan (RPJMD), reflecting the vision, mission, goals, and policy directives from the Jayawijaya Regent for the upcoming five years.

This analysis is also based on interviews with the Secretary, Head of Subdivision, and staff responsible for planning in the Planning, Data, and Reporting Subdivision of the Jayawijaya Inspectorate, where the head of the subdivision is serving as an acting official. Based on the data management results from the existing KPIs, a mapping was created, as shown in Figure 5.

c. ISO 27001:2013 Analysis

The analysis of the maturity level of the Information Security Management System (ISMS) based on the ISO 27001:2013 standard has been conducted through data collection from 10 respondents, including the leadership and staff of the Inspectorate. The assessment was carried out using a questionnaire that covers various information security controls in accordance with Annex A of ISO 27001, as shown in Table 8.

Based on the data analysis from the questionnaire, the average score for the maturity level of information security management at the Inspectorate of Jayawijaya is 2.97. This score indicates that the Inspectorate is currently at Level 3 – Defined, where information management processes are beginning to be well documented and consistently applied, but improvements are still needed to reach a higher level. From Table 8 the Annex A clauses of ISO 27001:2013 are presented in the maturity level graph shown in image 6.

The ISO 27001:2013 gap analysis reveals that the organization is at Level 3 (Defined), where security controls are defined and applied consistently. The target is Level 5 (Optimized), which involves

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

proactive and continuously improved control management. Table 7 outlines the gap, highlighting areas that need improvement to achieve full optimization.

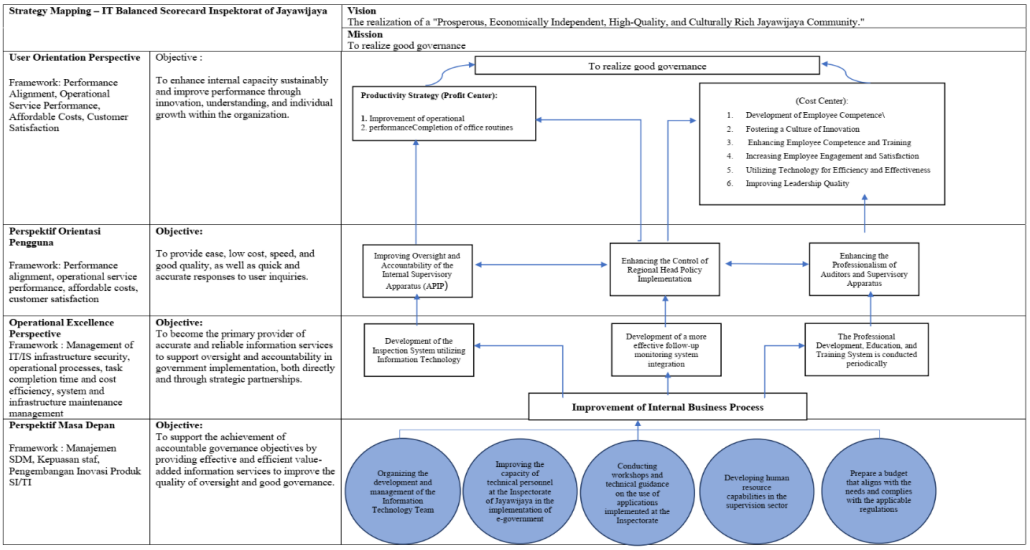

Figure 5 Vision, Mission, and Strategy Map of the Jayawijaya District Inspectorate with IT Balanced Scorecard

Table 8 ISO 27001:2013 Maturity Level

Annex A	***Score***	***Maturity Level***
A.5 Information security policies	*2,33*	*2 - Repeatable*
A.6 Organization of information security	*2,55*	*2 - Repeatable*
A.7 Human resource security	*4,01*	*4 - Managed*
A.8 Asset management	*2,68*	*2 - Repeatable*
A.9 Access control	*3,79*	*3 - Defined*
A.10 Cryptography	*0,90*	*1 - Non Existent*
A.11 Physical and environmental security	*2,78*	*2 - Repeatable*
A.12 Operation security	*2,94*	*2 - Repeatable*
A.13 Communication security	*3,29*	*3 - Defined*
A.14 System acquisition, development and maintenance	*2,53*	*2 - Repeatable*
A.15 Supplier relationships	*4,15*	*4 - Managed*
A.16 Information security incident management	*3,53*	*3 - Defined*
A.17 Information security aspects of business continuity management	*2,45*	*2 - Repeatable*
A.18 Compliance	*3,63*	*3 - Defined*
Average	***2,97***	***3 - Defined***

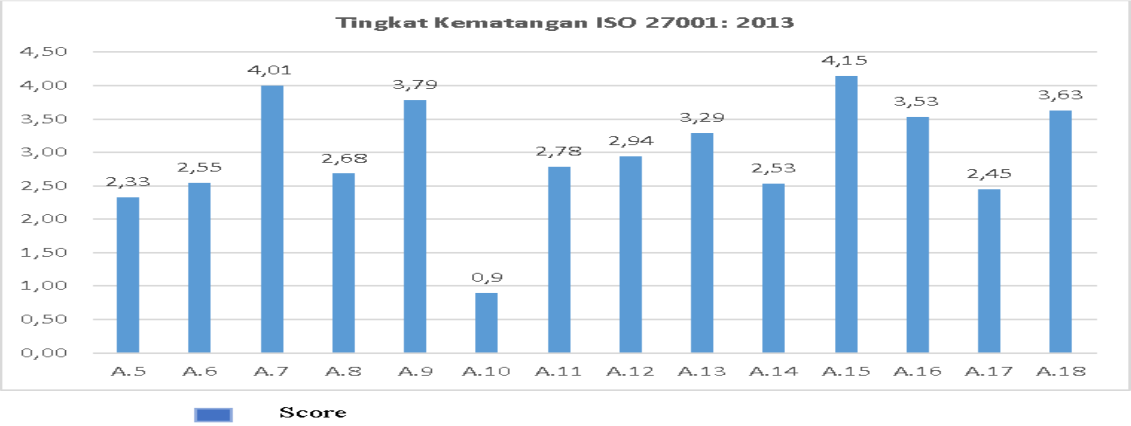

Figure 6 The maturity level graph of ISO 27001:2013

Tabel 9 Gap Analysis on ISO 27001:2013

Annex A	***Current Score***	***Maximum Score***	***Gap***
A.5 Information security policies	2,33	5	2,67
A.6 Organization of information security	2,55	5	2,45
A.7 Human resource security	4,01	5	0,99
A.8 Asset management	2,68	5	2,32
A.9 Access control	3,79	5	1,21
A.10 Cryptography	0,90	5	4,10
A.11 Physical and environmental security	2,78	5	2,22
A.12 Operation security	2,94	5	2,06
A.13 Communication security	3,29	5	1,71
A.14 System acquisition, development and maintenance	2,53	5	2,47
A.15 Supplier relationships	4,15	5	0,85
A.16 Information security incident management	3,53	5	1,47
A.17 Information security aspects of business continuity management	2,45	5	2,55
A.18 Compliance	3,63	5	1,35
Average	**2,97**	**5**	**2,03**

From the data above, the gap or difference between the actual condition and the desired condition regarding the maturity level of information security controls can be visualized. The maturity ratio ISO 27001:2013 is illustrated in Figure 7.

Analysis of Information Systems and Technology Requirements

In future business processes, it is crucial to map information needs to improve technology and systems at the Jayawijaya Regional Inspectorate. Based on gap analysis, the following actions can be taken:

1. Upgrade: Update existing systems to meet current standards.
2. Replace: Swap outdated systems with more efficient ones.
3. Continue as-is: Retain effective systems that align with future strategies.
4. New System: Implement entirely new systems, especially if current methods are manual.
5. Retire: Discontinue obsolete systems based on the business blueprint.

In addition to the gaps mentioned above, there are also gaps in information systems, technology, IT human resources, and IT/IS management. These are mapped in table 10.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

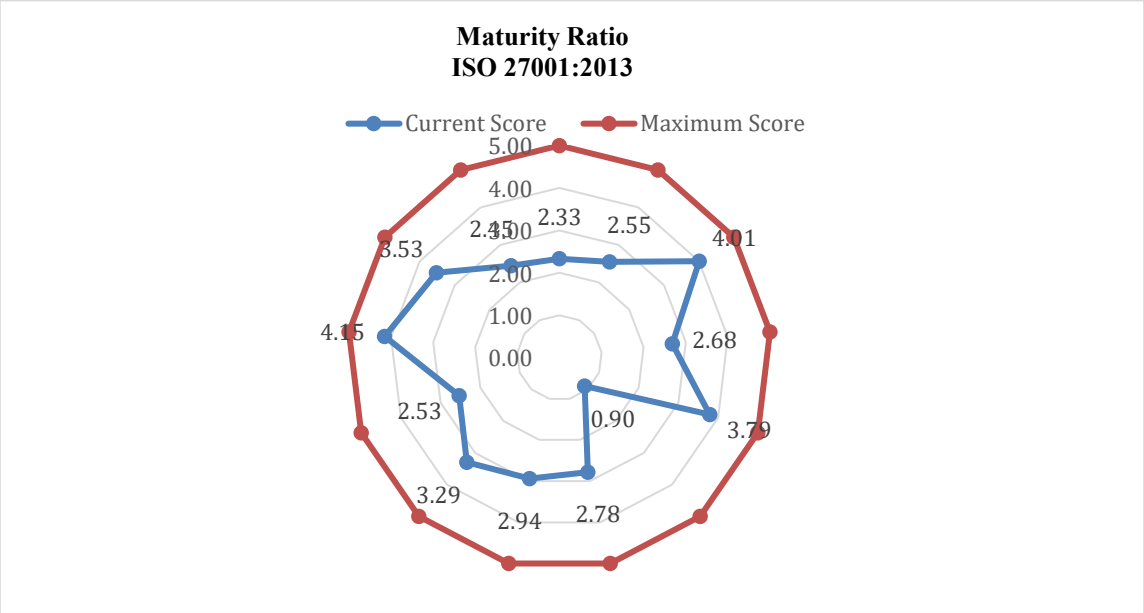

Figure 7 Maturity Ratio ISO 27001:2013

Table 10 Information dan Technology Needs Systems Gaps

Potential Business Needs	Current Conditions	Information System Needs	Recommended Actions
Integrated goods request system	Procurement process is not integrated with other systems	Integrated Asset Management System	Implement new system
Quick response to employee and public complaints	Complaints are handled manually via phone	Centralized Help Desk System	Implement new system
Employee competency development	No application for tracking competencies	Human Resource Management System	System upgrade
Reward and punishment guidelines	Manual evaluation for awards and sanctions	Reward & Punishment Module	Implement new system
Structured employee performance assessment	Performance evaluation depends on attendance	KPI-based Performance Evaluation System	Implement new system
Integrated management reports	Integrated management reports	Business Intelligence (BI)	Implement new system
Asset and goods inventory	Inventory is done manually using spreadsheets	Integrated Inventory Management System	Implement new system
Improved Network Cable Quality	Many network cables still use CAT-5 standard	CAT-6 Cables	Upgrade
Guaranteed Database Backup System	Data backup is done manually and stored on local servers	Automated Backup System	Implement new system
Centralized Antivirus	Antivirus is installed	Antivirus Server	Implement new

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Potential Business Needs	Current Conditions	Information System Needs	Recommended Actions
Management	locally on each computer		system
Web Server untuk Hosting Portal Informasi dan Transparansi	Inspectorate portal is still hosted by an external party	Internal Web Server	Implement new system
Increased IT HR Competency	Limited personnel and soft skills in IT staff	IT Workshops	Implement new system
Standard Operating Procedures (SOP)	No SOP for IT operations	Development of IT SOP	Implement new system
IT Governance	No IT governance framework	IT Governance Framework	Implement new system
IT Master Plan Development	No IT Master Plan	IT Master Plan Development	Implement new system
Strategic SI/TI Development Planning	No strategic planning for SI/TI	SI/TI Strategic Planning	Implement new system
Software and Tools Standardization for Integrated Applications	No standard for software and tools used	Software and Tools Standardization	Implement new system

Strategy Formulation Stage

The strategy formulation stage is conducted to design concrete steps that will enhance the information systems, management, and operational capabilities of the Jayawijaya Inspectorate. By formulating the right strategies, the Inspectorate can achieve better operational efficiency, improve service quality, and strengthen security as well as data management. This strategy formulation also aims to ensure that the technology used can support transparency, accountability, and the smooth conduct of oversight and reporting activities. Table 11 illustrates the strategic actions to be implemented in order to improve the IT systems at the Jayawijaya Inspectorate, focusing on operational efficiency, service quality, security, data management, and the development of IT human resources. All of these actions are intended to support enhanced oversight, increased transparency, and improved organizational performance through technology.

Table 11 Strategy Formulation Stage

Strategy Area	Strategy	Description
Business IT Strategy	Operational Efficiency	Implement integrated e-audit and automated reporting systems for streamlined oversight and evaluation
	Service Quality Improvement	Develop online portals and mobile applications for public access to audit information, increasing transparency
	Data Management Optimization	Use centralized data management and big data analytics for efficient access and in-depth analysis of audit data.

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	Enhanced Security	Enforce robust security policies, including encryption, access control, and cybersecurity monitoring
	Collaboration & Partnerships	Partner with reputable IT service providers and collaborate with other agencies to support transparency and efficiency
IT Management Strategy	Human Resource Development	Identify critical skill requirements and provide training for IT staff to address technical, managerial, and security needs.
	Information Security Policy	Implement comprehensive policies for managing system security, privacy, and reliability.
	Data Governance & Risk Management	Data Governance & Risk Management
IT Strategy	Platform & Technology Selection	Conduct a thorough assessment to select scalable, secure technology that aligns with Inspectorate requirements.
	Infrastructure Planning	Design robust infrastructure (e.g., communication networks, servers, data storage) to support operations and growth
	Scalable IT Architecture	Develop adaptable IT architecture that can accommodate new functionalities without disrupting current systems

Determining the Future Application Portfolio

Based on the results of the previous mapping, an analysis of the contributions of each technology, application, and even available resources at the Inspectorate, both currently and in the future, is conducted. The proposed application portfolio is divided into four categories according to the McFarlan Grid model, namely: Strategic, High Potential, Key Operational, and Support. The proposed portfolio consists of 2 strategic applications, 4 high-potential applications, 2 key operational applications, and 2 support applications. The outcomes of the strategic IS planning are mapped into the following portfolio (Table 12).

The following IT network requirements are proposed to support operational needs and align with business and IT strategies, as shown in table 13. Additionally, proposed Human Resource Development (HRD) strategies for the Inspectorate are outlined in table 14, aimed at enhancing workforce competence, productivity, and efficiency.

Table 12 Determining the Future Application Portfolio

Strategic	***High Potensial***
- SIMADU - SI Alan	- Inspektorat *Mobile App* - SI Planning - SI Administrasi - E- PKPT
Key Potential	***Support***

Journal of Information Systems Engineering and Management
2025, 10(54s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- *Website* Inspektorat - SI SDM	- SI Manset - SI Absensi

Table 13 Proposed Information Technology Portfolio

Component	Details
Network Infrastructure	Switches and Routers: Managed switches for network management, VLAN support for network segmentation; routers with firewall capabilities for added security
Network Topology	Star Topology: Central switch connection for all devices, allowing easier management and troubleshooting. VLAN segmentation and wireless isolation for traffic control.
Network Security	Firewall: Hardware and software firewalls to protect against external threats; VPN implementation for secure remote access for staff.
Capacity and Scalability	Bandwidth: Sufficient to support web-based applications, internal communication, and cloud services access. Scalable Infrastructure to accommodate organizational growth
Backup Internet Service	Starlink Internet: Backup internet service through Starlink to ensure continuity in case of disruptions in the government-provided internet service.

Table 14 Proposed Human Resource Development for the Inspectorate

Development Area	Initiatives
Technical Training & Education	- Training in modern audit techniques, digital audit tools, and supervisory methodologies. - Training on information system management, cybersecurity, and relevant software applications. - Training on recent government regulations, anti-corruption policies, and good governance practices.
Advanced Education & Certification	- Encourage staff to earn professional certifications, e.g., Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA). - Provide scholarships or support for advanced degrees (master's or doctoral programs) in relevant fields.
Recruitment & Staffing	Recruit new staff to fill vacant positions and address any staffing gaps

CONCLUSION

Through IT Balanced Scorecard, SWOT analysis, and ISO 27001 review, it is determined that Jayawijaya Inspectorate's strengths lie in leadership support and basic IT infrastructure. However, the main weaknesses are limited human resources, insufficient IT infrastructure, and the absence of a dedicated technical team. Growth opportunities include government policy support, though challenges such as frequent regulatory changes and rapid technological advancements pose significant threats.

Research Article

The ISO 27001:2013 standard implementation shows that Jayawijaya Inspectorate's information maturity level has reached level 3, indicating that information security is planned, monitored, adjusted, and well-documented.

To further enhance the maturity level and future capability of APIP, strategic planning based on SWOT analysis, IT Balanced Scorecard, and ISO 27001 standards is recommended. The primary focus should be on strengthening human resource capacity through training, implementing integrated monitoring technology, and developing an accountability dashboard. These efforts aim to improve oversight performance, accountability, and data security within the Inspectorate.

Acknowledgements

We would like to express our greatest appreciation to the Lembaga Pengelola Dana Pendidikan (LPDP) for providing financial support, which made this study possible. Their contributions have been instrumental in the successful completion of this research.

REFERENCES

[1] Aini, Q., Cahya Wasiqi, N., Fitra Alfajri, M., Ulinnuha, Z., Kurnia Purwati, Y., Kusuma Ayu, I., & Aurora Yasmin, N. (2024). RISK ASSESSMENT MATURITY LEVEL OF ACADEMIC INFORMATION SYSTEM USING ISO 27001 SYSTEM SECURITY ENGINEERING-CAPABILITY MATURITY MODEL. In *Journal of Applied Engineering and Technological Science* (Vol. 5, Issue 2).

[2] Almeida, R., Lourinho, R., Da Silva, M. M., & Pereira, R. (2018). A model for assessing COBIT 5 and ISO 27001 simultaneously. *Proceeding - 2018 20th IEEE International Conference on Business Informatics, CBI 2018*, *1*, 60–69. https://doi.org/10.1109/CBI.2018.00016

[3] Amega, K., Moumouni, Y., Laré, Y., Bhandari, R., Takouda, P., & Madougou, S. (2024). Power system transformation in emerging countries: A SWOT/PESTLE analysis approach towards resiliency and reliability. *Heliyon*, *10*(12). https://doi.org/10.1016/j.heliyon.2024.e33018

[4] Anjeli, D., Faulina, T., Fakih, A., Informatika, J., & Komputer, D. (2022). Sistem Informasi Perpustakaan Sekolah Dasar Negeri 49 OKU Menggunakan Embarcadero XE2 Berbasis Client Server. In *JIK* (Vol. 13, Issue 2).

[5] Antunes, A. L., Cardoso, E., & Barateiro, J. (2024). The Balanced Scorecard Ontology: A Semantic Approach to Enhance Strategy Management. *IEEE Engineering Management Review*. https://doi.org/10.1109/EMR.2024.3439880

[6] Calder, A., & Watkins, S. (2016). *IT Governance an International Guide to Data Security and ISO 27001/ISO27002* (Vol. 6th). Kogan Page.

[7] Clarissa, S., & Wang, G. (2023). Assessing Information Security Management Using ISO 27001:2013. *Jurnal Indonesia Sosial Teknologi*, *4*(9), 1361–1371. https://doi.org/10.59141/jist.v4i9.739

[8] Deni Wahyudi, M., & Rasid Ridho, M. (2019). *SISTEM INFORMASI PENJUALAN MOBIL BEKAS BERBASIS WEB PADA CV PHUTU OIL CLUB DI KOTA BATAM*.

[9] Eas Certification team. (2023). *Prinsip Keamanan Informasi ISO 27001 - CIA Triad*. Eas Certification. . https://ekualindo.com/prinsip-keamanan-informasi-iso-27001/

[10] Freddy Rangkuti. (2006). *Analisis SWOT Teknik Membedah Kasus Bisnis* (14th ed., Vol. 21). PT. Gramedia Pustaka Utama. https://books.google.co.id/books?id=UHV8Z2SE57EC&printsec=frontcover&hl=id#v=onepage&q&f=false

[11] Gazi, F., Atan, T., & Kılıç, M. (2022). The Assessment of Internal Indicators on The Balanced Scorecard Measures of Sustainability. *Sustainability (Switzerland)*, *14*(14). https://doi.org/10.3390/su14148595

[12] Grembergen, W. V, & Saull, R. (2001). AligningBusiness and Information Technology through theBalanced Scorecard at a Major Canadian FinancialGroup: its Status Measured with an IT BSC Maturity Model. *AligningBusiness and Information Technology through TheBalanced Scorecard at a Major Canadian FinancialGroup: Its Status Measured with an IT BSC Maturity Model*.

[13] Haag, S., & Keen, P. G. W. (1996). *Information Technology: Tomorrow's Advantage Today, Mcgraw-Hill College*. Hammond: Mcgraw-Hill College.

[14] IMF. (2017). *The IMF and Good Governance*. https://www.imf.org/en/About/Factsheets/Sheets/2023/The-IMF-and-Good-Governance

[15] Kaplan, R. S., & Norton, D. P. (1996). *The Balanced Scorecard: Translating Strategy Into Action*.

Harvard Business School Press.

[16] Kerzner, Harold., & Saladis, F. P. (2009). *Project management workbook and PMP/CAPM exam study guide*. J. Wiley & Sons.

[17] Komite Nasional Kebijakan Governansi. (2022). *DRAF 26 DESEMBER 2021 PEDOMAN UMUM GOVERNANSI SEKTOR PUBLIK INDONESIA (PUG-SPI)*.

[18] Maranjaya. (2022). *Good Governance Sebagai Tolak Ukur Untuk Mengukur Kinerja Pemerintahan*.

[19] Nicho, M., & Muamaar, S. (2016). Towards a Taxonomy of Challenges in an Integrated IT Governance Framework Implementation. *Journal of International Technology and Information Management*, *25*(2). https://doi.org/10.58729/1941-6679.1266

[20] Oktari, R. S., Latuamury, B., Idroes, R., Sofyan, H., & Munadi, K. (2023). Knowledge management strategy for managing disaster and the COVID-19 pandemic in Indonesia: SWOT analysis based on the analytic network process. *International Journal of Disaster Risk Reduction*, *85*. https://doi.org/10.1016/j.ijdrr.2022.103503

[21] Pham, L.-H. T., Desai-Naik, T., Hammond, L., & Abdeljabbar, W. (2023). *INFORMATION SYSTEMS FOR BUSINESS*. https://LibreTexts.org

[22] Prabowo Wahyu, A., & Ramadhani, R. D. (2021, February). *Perancangan Contingency Planning Disaster Recovery Unit Teknologi Informasi menggunakan NIST SP800-34*. LPPM UDINUS.

[23] Puskum dan Humas BPN RI. (2014). *Undang-Undang Republik Indonesia Nomor 23 Tahun 2014 tentang Pemerintah Daerah*.

[24] Putra, P. A., & Soewito, B. (2021, November 17). *Pentingnya ISO 27001 sebagai Standard Keamanan Informasi didalam Perusahaan*. BINUS Higher Education.

[25] Renaldo, N. (2022). Journal of Applied Business and Technology Benefits and Challenges of Technology and Information Systems on Performance. In *Journal of Applied Business and Technology (JABT)* (Vol. 2022, Issue 3). www.e-jabt.org

[26] Rossieta, H., Muktiyanto, A., & Ira Geraldina, Ms. (2022). *Modul 1 Definisi Tata Kelola dalam Entitas Sektor Publik*.

[27] Savić, Z., & Huđekr, M. (2023). BALANCED SCORECARD BASED APPROACH IN MODELING A BUSINESS INTELLIGENCE SYSTEM. *Social Informatics Journal*, *2*(2), 37–48. https://doi.org/10.58898/sij.v2i2.37-48

[28] Selay, A., Andgha, G. D., Alfarizi, M. A., Izdhihar, M., Wahyudi, B., Falah, M. N., Encep, M., & Khaira, M. (2023). SISTEM INFORMASI PENJUALAN. In *Karimah Tauhid* (Vol. 2, Issue 1).

[29] Setyadi, R. (2021, March 16). *Paradigma Baru Pengawasan: APIP Sebagai "Strategic Partner."* Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi - Republik Indonesia.

[30] Usman, A., Selvi, F., Ningsih, L., & Reskiana Putri, D. (2023). *The Implementation Of Balanced Scorecard In Indonesian Companies Companies: A Systematic Literature Review*.

[31] Vladimir Zwass. (2024). information system. In The Editors of Encyclopaedia Brittania (Ed.), *Britanica* (Information System, Vol. 1, pp. 1–1). https://www.britannica.com/. https://www.britannica.com/topic/information-system

[32] Ward, J., & Peppard, J. (2002). *Strategic Planning for Information Systems: Vol. 640 pp* (3rd Edition,). John Wiley & Sons Ltd.