Enchancing IT Governance at BPS Manado: A COBIT 2019 Framework Implementation Study

George Morris William Tangka*[1], Erienika Lompoliu[2]
[1,2]Universitas Klabat; Airmadidi, Sulawesi Utara
[1]Fakultas Ilmu Komputer, Universitas Klabat
[2]Fakultas Ekonomi dan Bisnis, Universitas Klabat
e-mail: *[1]gtangka@unklab.ac.id, [2]erienika.lompoliu@unklab.ac.id

Abstract

Information Technology (IT) governance is a framework used by organizations to effectively manage and control their information technology resources, aiming to maximize business value. The Central Statistics Agency (BPS), in its responsibility to provide critical data, faces challenges in optimizing their IT management. This research aims to apply the COBIT 2019 framework as a structure to improve Information Technology (IT) governance at BPS, facilitating efficient and smooth management of critical data services. The findings of this research reveal that BPS has not carried out a comprehensive assessment of Information Technology (IT) governance. Apart from that, there are challenges in managing order data and stock information. In addition, BPS requires a more structured information technology governance process to ensure targeted and effective use of technology, so that companies can achieve their goals more efficiently. The literature review process helps in identifying gaps in current research, paving the way for more comprehensive and insightful research. After conducting calculations for the analysis of objectives APO13 and DSS04, different results were obtained. In APO13, the questions asked only reached level 3, which means it stopped below 85%, specifically at 66%. Meanwhile, in DSS04 the questions asked continued up to the last level with a consistently high percentage, above 85%. By integrating these findings into the research, this study becomes enriched with a strong theoretical foundation, ensuring an in-depth and rigorous analysis of this issue.

Keywords: *Information Technology Governance (ITG), COBIT 2019, Data Service Management*

Peningkatan Tata Kelola TI di BPS Manado: Kajian Implementasi Framework COBIT 2019

Abstrak

Tata kelola Teknologi Informasi (TI) adalah kerangka kerja yang digunakan oleh organisasi untuk mengelola dan mengendalikan sumber daya teknologi informasi mereka secara efektif, dengan tujuan untuk memaksimalkan nilai bisnis. Badan Pusat Statistik (BPS), dalam tanggung jawabnya untuk menyediakan data-data penting, menghadapi tantangan dalam mengoptimalkan manajemen TI mereka. Penelitian ini bertujuan untuk menerapkan kerangka kerja COBIT 2019 sebagai struktur untuk meningkatkan tata kelola Teknologi Informasi (TI) di BPS, memfasilitasi manajemen layanan data penting yang efisien dan lancar. Temuan dari penelitian ini mengungkapkan bahwa BPS belum melakukan penilaian menyeluruh terhadap tata kelola Teknologi Informasi (TI). Selain itu, terdapat tantangan dalam mengelola data pesanan dan informasi stok. Selain itu, BPS memerlukan proses tata kelola teknologi informasi yang lebih terstruktur untuk memastikan penggunaan teknologi yang ditargetkan dan efektif, sehingga perusahaan dapat mencapai tujuan mereka dengan lebih efisien. Proses tinjauan literatur membantu dalam mengidentifikasi kesenjangan dalam penelitian saat ini, membuka jalan bagi penelitian yang lebih komprehensif dan mendalam. Setelah melakukan perhitungan untuk analisis tujuan APO13 dan DSS04, didapatkan hasil yang berbeda. Pada APO13, pertanyaan yang diajukan hanya mencapai level 3, yang berarti berhenti di bawah 85%, khususnya pada 66%. Sementara itu, pada DSS04 pertanyaan yang diajukan terus hingga level terakhir dengan persentase yang konsisten tinggi, di atas 85%. Dengan mengintegrasikan temuan ini ke dalam penelitian, studi ini menjadi lebih kaya dengan dasar teoritis yang kuat, memastikan analisis yang mendalam dan ketat terhadap masalah ini.

Kata Kunci: Tata Kelola TI, COBIT 2019, Manajemen Layanan Data

1. Introduction

Technology continues to redefine the way we live, work, and interact, continually pushing the boundaries of what is possible. As time advances, the progress in technology and information opens up greater opportunities. This leads to increased productivity for companies when they use information technology [1]. One of the organizations utilizing Information Technology is the government agency, the Badan Pusat Statistik (BPS). Information Technology (IT) has become a crucial component for today's statistical center services. As an institution providing statistical data services, they must have an IT system that is well-function and can be managed effectively. To get the best outcomes from using information technology, organizations such as BPS also need to embrace and apply suitable frameworks in managing their IT [2].

Technology continues to reshape our lives, work, and interactions, opening up new possibilities and enhancing productivity [1]. Organizations, such as the government agency Badan Pusat Statistik (BPS) in Indonesia, recognize the pivotal role of Information Technology (IT) in delivering efficient services [2]. Effective IT governance is crucial for aligning IT with organizational goals, managing risks, and ensuring compliance with regulations [3]. To achieve this, organizations often adopt frameworks like Control Objectives for Information and related Technology (COBIT) 2019 [4].

COBIT 2019, developed by ISACA and ITGI, serves as a comprehensive guide for IT governance, assisting organizations in maximizing IT investments and bridging the gap between business risks and IT implementation [5]. Implementing COBIT 2019 is particularly important for BPS to enhance IT governance, improve IT risk management, operational efficiency, information security, and decision-making [6]. This study aims to apply the COBIT 2019 framework to BPS to facilitate efficient IT management [7]. In this research, BPS's IT governance maturity will be assessed using design factors from the COBIT 2019 framework.

The study will evaluate BPS's IT governance maturity by considering various design factors outlined in the COBIT 2019 framework [8]. These factors include enterprise strategy [9], enterprise goals, IT risk profile, IT-related issues, threat landscape, compliance requirements, role of IT, sourcing model of IT, IT implementation methods, and technology adoption strategy. By analyzing these design factors, the research will provide insights into optimizing IT governance at BPS and offer actionable recommendations for improvement [9].

2. Research Method

The research followed several stages as illustrated in Figure 1. In the problem identification stage, interviews were conducted with Badan Pusat Statistik (BPS) to understand its profile, objectives, and IT implementation status. The findings revealed that BPS lacks a comprehensive assessment of its IT governance and faces challenges in managing order data and stock information. Thus, a structured IT governance process is needed to ensure effective technology use and goal achievement.

To address these challenges, effective strategies for assessing and enhancing technology usage are crucial for BPS. Implementing a comprehensive IT governance framework will optimize operations, align technology with organizational goals, and improve efficiency and accuracy in managing orders and stock data. The research also involved a literature review to identify relevant theories and academic articles related to IT governance, providing a solid theoretical foundation and insights for a deeper understanding of the problem.

In the analysis phase, the Workflow Governance System Design in COBIT 2019 was used for assessment, covering aspects like context, strategy, and the company's business environment. This evaluation helped understand BPS's plans, assess the extent of technology implementation, and identify technological needs for implementing IT governance effectively.

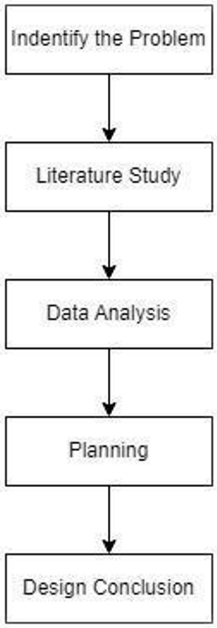

Figure 1 Research Flow

3. Results and Discussion

3.1 Design Factor 1 (Enterprise Strategy)

The most crucial aspect at the North Sulawesi Central Statistical Agency is the Client Service/Stability section. This reflects the agency's priority of providing services to the public, as the BPS primarily focuses on serving the community.

3.2 Design Factor 2 (Enterprise Goals)

The assessment highlights several key areas crucial for the BPS. EG01 emphasizes the importance of the Portfolio of Competitive Products and Services, scoring a 5 due to BPS's main reliance on its publication portfolio, encompassing all its work and results. Similarly, EG02's Managed Business Risk scores 5, reflecting BPS's data-centric nature and the need for robust data protection and hardware maintenance. Compliance with External Laws and Regulations in EG03 also scores high, emphasizing BPS's role in data oversight and adherence to regulations. EG04 to EG06 focus on Financial Information, Customer Service Culture, and Business Continuity, all scoring 5 due to BPS's reliance on funds, community service focus, and heavy data usage.

The remaining areas, from EG07 to EG13, further underscore BPS's reliance on information systems, the importance of staff motivation and skills, and the value of digital transformation and innovation. Topics like Quality of Management Information, Optimization of Internal Business Processes, and Business Process Costs all score high due to BPS's dependence on updated systems and cost considerations. Staff motivation and compliance with internal policies are crucial, scoring 5, reflecting the significance of motivated staff and adherence to rules. Lastly, Digital Transformation Programs score high, reflecting the potential benefits of simplifying tasks and cost-saving.

3.3 Design Factor 3 (Risk Profile)

Based on interviews with the North Sulawesi BPS Office, several impacts and their likelihoods were identified. IT investment decision-making and portfolio maintenance scored a 2, indicating rare but significant failures. Program and Project Lifecycle management scored a 5, reflecting potential chaos when staff cannot manage tasks outside their expertise, although this is less likely due to BPS's training programs. IT Cost & Oversight and IT Expertise both scored 1, suggesting that budget shortages and staff skills have minimal impact due to BPS's strong internet facilities and training initiatives.

Enterprise/IT Architecture scored a 3, indicating challenges in learning new applications, yet BPS's thorough testing ensures functionality. IT Operational Infrastructure Incidents and Unauthorized Actions both scored 5, reflecting past failures and potential disruptions from IT equipment damage or software issues. Software Adoption/Usage Problems scored 4, indicating the impact of outdated software, but BPS's frequent updates mitigate this risk. Logical Attacks scored 5, reflecting the significant impact of cyberattacks despite their low likelihood due to increased security measures. Third Party/Supplier Incidents and Noncompliance both scored 4, indicating challenges with external partners and occasional procedural noncompliance. Geopolitical Issues scored 1, suggesting minimal influence on BPS's data production. Industrial Action and Acts of Nature scored 5, reflecting potential disruptions from work concentration and natural disasters. Technology-based Innovation and Environmental Factors scored 5 and 4, respectively, with low likelihoods due to BPS's rigorous testing and past infrastructure issues. Data and Information Management scored 5, indicating the significant impact of data leaks given BPS's reliance on data.

3.4 Design Factor 4 (Related Issue)

BPS North Sulawesi faces critical IT challenges that impact its operations and stakeholder trust. Data leaks pose a significant threat due to BPS's heavy reliance on data integrity. Dissatisfaction with IT service quality and inconsistent service from outsourcing partners further strain BPS's IT landscape. Additionally, serious IT incidents like data loss, security breaches, and application errors disrupt operations and require immediate attention. Issues with contract fulfillment by partners also need addressing to ensure compliance with agreed terms.

Despite these challenges, BPS maintains transparent IT spending without hidden costs, though project overlap and resource inefficiencies, like lack of IT staff and skills, persist. While company executives are involved in IT matters, they balance multiple responsibilities. High IT costs are managed by the finance department, and the IT model's complexity is mitigated by structured explanations from the BPS Head.

On a positive note, BPS successfully adopts new technology through trial processes, ensures effective communication between IT and non-IT staff, and maintains data quality and online accessibility. Centralized application sourcing involves business departments without sidelining IT, and BPS upholds security and privacy regulations. Despite occasional challenges with new technology, BPS views them as manageable issues. These insights highlight both the challenges and opportunities BPS North Sulawesi faces in IT management, guiding efforts to enhance operational efficiency and performance.

3.5 Design Factor 5 (Threat Landscape)

Implementing the COBIT framework for IT governance at BPS North Sulawesi highlights the critical importance of managing the IT threat landscape. The framework categorizes threats into two levels: "High" with 100% importance and "Normal" with 0%. Given BPS's primary focus on statistical data and the sensitivity of the data they manage, safeguarding against high-level threats is paramount. This commitment is demonstrated through robust security measures, continuous monitoring, and incident response plans aimed at mitigating high-level IT threats. While normal-level threats are rated at 0% importance, they still require attention. Rigorous risk management and ongoing monitoring are essential to prevent these threats from escalating over time.

In essence, the IT Threat Landscape table underscores the crucial role of data protection and IT security in BPS North Sulawesi's IT governance framework. It aligns with the principles of the COBIT framework and underscores the organization's dedication to safeguarding its valuable data assets.

3.6 Design Factor 6 (Compliance Requirement)

The Compliance Requirements Table for implementing the COBIT framework at BPS North Sulawesi prioritizes IT security as High (10%), reflecting the agency's commitment to safeguarding its data. Financial and administrative requirements are categorized as Normal (50%), while external sector impacts are deemed Low (40%). This categorization guides the organization in allocating resources effectively, emphasizing data integrity and IT security as top priorities.

3.7 Design Factor 7 (Role of IT)

The "Role of IT" table based on COBIT 2019 for BPS Sulawesi Utara highlights IT's varied roles. IT is primarily seen as a support function (Importance 2) during data collection, assisting external partners using BPS applications. While IT issues can disrupt business processes (Importance 5), IT isn't seen as driving innovation in business operations. It serves as an innovation catalyst (Importance 2) but isn't considered a critical dependency for business continuity. Yet, IT's significance is evident in data collection and management (Importance 5), playing a crucial role in both business processes and innovation. This understanding guides IT governance and resource allocation within the organization.

3.8 Design Factor 8 (Sourcing Model of IT)

In implementing COBIT 2019 at BPS North Sulawesi, there's a strong focus on using internal resources for IT services, given a 100% importance rating. The organization places no value on outsourcing or cloud-based IT solutions, preferring to manage IT functions internally to maintain data security. This commitment to insourcing underscores their dedication to data security and aligns with the principles of the COBIT framework, guiding their IT resource selection based on data security priorities.

3.9 Design Factor 9 (IT Implementation Method)

IT implementation methods, as outlined in the COBIT 2019 framework, include three main points, namely "agile," "devops," and "traditional." In the context of BPS (Central Statistics Agency) of North Sulawesi, the interview results show that questions related to IT implementation methods are more technical questions. Therefore, an answer to this question cannot be provided due to limited information resources. The people interviewed in this study were not individuals directly associated with IT or application development within the organization.

3.10 Design Factor 10 (Technology Adaption Strategy)

In the context of BPS North Sulawesi's IT implementation methods, three main approaches were identified through interviews:

- First Mover (20%): BPS North Sulawesi adopts this approach as early adopters, creating custom applications to gain a competitive edge. They are willing to take risks to be among the first to implement new technologies.
- Follower (80%): BPS North Sulawesi adopts this approach as early adopters, creating custom applications to gain a competitive edge. They are willing to take risks to be among the first to implement new technologies.
- Slow Adopter (Slow Approach - 0%): BPS North Sulawesi adopts this approach as early adopters, creating custom applications to gain a competitive edge. They are willing to take risks to be among the first to implement new technologies.

The organization prioritizes the "Follower" approach, emphasizing caution in technology adoption while leveraging the "First Mover" approach for custom solutions. This strategy aligns with their selective adoption of mature and impactful technologies, guiding their IT strategy to meet business goals effectively.

3.11 Determination of Priority Processes

After evaluating ten design factors at the Central Statistics Agency with the COBIT 2019 framework, processes with importance levels over 75, like APO13 - Managed Security and DSS04 - Manage Continuity, aim for capability level 4. These two processes will undergo further evaluation through interviews with the IT Supervisor to assess the agency's IT governance capability and ensure it meets the desired level.

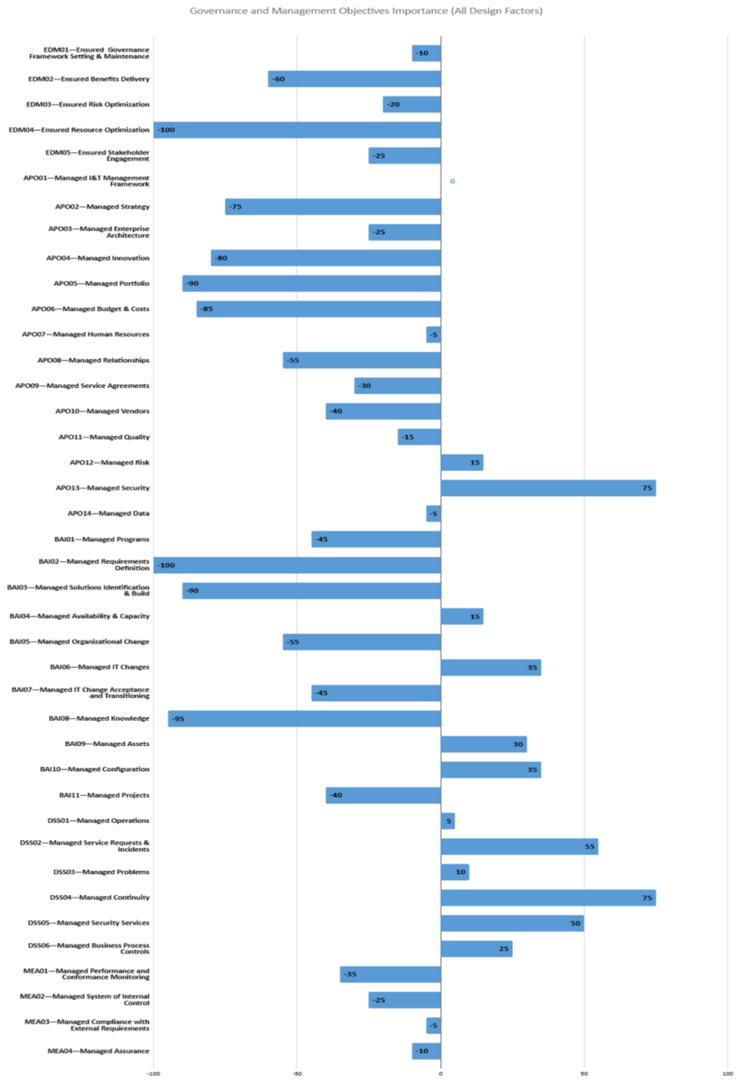

Figure 2 Governance and Management Objectives Importance

3.12 APO13 – Manage Security Level 2

Table 1 APO13 Level 2 Activities

No	Sub Process	Question	Yes/No
1	APO13.01 Estabilish and maintain an information security	Define the scope and boundaries of the information security management system (ISMS) in terms of the characteristics of the enterprise, the organization, its location, assets and	☑

	management system (SMS).	technology. Include details of, and justification for, any exclusions from the scope.	
2	APO13.01 Estabilish and maintain an information security management system (SMS).	Define an ISMS in accordance with enterprise policy and the context in which the enterprise operates.	☑
3	APO13.01 Estabilish and maintain an information security management system (SMS).	Align the ISMS with the overall enterprise approach to the management of security.	☑
4	APO13.01 Estabilish and maintain an information security management system (SMS).	Obtain management authorization to implement and operate or change the ISMS	☑
5	APO13.01 Estabilish and maintain an information security management system (SMS).	Prepare and maintain a statement of applicability that describes the scope of the ISMS.	☑
6	APO13.01 Estabilish and maintain an information security management system (SMS).	Define and communicate Information security management roles and responsibilities.	☑
7	APO13.01 Estabilish and maintain an information security management system (SMS).	Communicate the ISMS approach	☑

The table of level 2 subprocesses was evaluated using a formula to determine if they meet the "F - fully achieved" criteria according to the NPLF method. The capability result was 100%, indicating that all activities at level 2 have been satisfactorily met, allowing progression to the next level.

3.13 APO13 – Manage Security Level 3

Table 2 APO13 Level 3 Activities

No	Sub Process	Question	Yes/No
1	APO013.02 Define and manage an information security and privacy risk treatment plan.	Formulate and maintain an information security risk treatment plan aligned with strategic objectives and the enterprise architecture. Ensure that the plan identifies the appropriate and optimal management practices and security solutions, with associated resources, responsibilities and priorities for managing identified information security risk.	☑
2	APO013.02 Define and manage an information security	Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage security related risk.	☑

	and privacy risk treatment plan.		
3	APO013.02 Define and manage an information security and privacy risk treatment plan.	Develop proposals to implement the information security risk treatment plan, supported by suitable business cases that include consideration of funding and allocation of roles and responsibilities.	☒
4	APO013.02 Define and manage an information security and privacy risk treatment plan.	Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan	☑
5	APO013.02 Define and manage an information security and privacy risk treatment plan.	Implement information security and privacy training and awareness programs.	☒
6	APO013.02 Define and manage an information security and privacy risk treatment plan.	Integrate the planning, design, implementation and monitoring of information security and privacy procedures and other controls capable of enabling prompt prevention, detection of security events, and response to security incidents.	☑

The capability process calculation yielded a result of 66%, placing all process activities at level 3 in the "Largely Achieved" category. Therefore, no further assessments or interviews for the next level are required.

3.14 DSS04 – Manage Continuity Level 2

Table 3 DSS04 Level 2 Activities

No	Sub Process	Question	Yes/No
1	DSS04.01 Define the business continuity policy, objectives and scope.	Identify internal and outsourced business processes and service activities that are critical to the enterprise operations or necessary to meet legal and/or contractual obligations.	☑
2	DSS04.01 Define the business continuity policy, objectives and scope.	Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.	☑
3	DSS04.01 Define the business continuity policy, objectives and scope.	Define and document the agreed minimum policy objectives and scope for business resilience.	☑
4	DSS04.01 Define the business continuity policy, objectives and scope.	Identify essential supporting business processes and related I&T services.	☑
5	DSS04.02 Maintain business resilience.	Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.	☑

6	DSS04.02 Maintain business resilience	Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.	☑
7	DSS04.02 Maintain business resilience	Establish the minimum time required to recover a business process and supporting I&T, based on an acceptable length of business interruption and maximum tolerable outage.	☑
8	DSS04.02 Maintain business resilience	Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.	☑
9	DSS04.03 Develop and implement a business continuity response.	Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.	☑
10	DSS04.03 Develop and implement a business continuity response.	Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.	☑
11	DSS04.03 Develop and implement a business continuity response.	Define the conditions and recovery procedures that would enable resumption of business processing. Include updating and reconciliation of information databases to preserve information integrity.	☑
12	DSS04.03 Develop and implement a business continuity response.	Develop and maintain operational BCPs and DRPs that contain the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements. Include links to plans of outsourced service providers	☑
13	DSS04.03 Develop and implement a business continuity response.	Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.	☑
14	DSS04.03 Develop and implement a business continuity response.	Define and document the information backup requirements required to support the plans. Include plans and paper documents as well as data files. Consider the need for security and off-site storage.	☑
15	DSS04.03 Develop and implement a business continuity response.	Determine required skills for individuals involved in executing the plan and procedures.	☑
16	DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).	Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP and DRP in meeting business risk.	☑
17	DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).	Define and agree on stakeholder exercises that are realistic and validate continuity procedures. Include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.	☑

18	DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).	Assign roles and responsibilities for performing continuity plan exercises and tests.	☑
19	DSS04.06 Conduct continuity plan training.	Roll out BCP and DRP awareness and training.	☒
20	DSS04.07 Manage backup arrangements.	Back up systems, applications, data and documentation according to a defined schedule. Consider frequency (monthly, weekly, daily, etc.), mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention), type of backup (e.g., full vs. incremental), and type of media. Consider also automated online backups, data types (e.g., voice, optical), creation of logs, critical end-user computing data (e.g., spreadsheets), physical and logical location of data sources, security and access rights, and encryption.	☑
21	DSS04.07 Manage backup arrangements.	Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.	☑
22	DSS04.07 Manage backup arrangements.	Periodically test and refresh archived and backup data.	☑
23	DSS04.07 Manage backup arrangements.	Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.	☑

Out of around 23 questions assessed, 22 have been addressed or implemented by the company, resulting in a 95% completion rate. Based on this high percentage, the company should proceed to the next level to achieve more concrete results.

3.15 DSS04 – Manage Continuity Level 3

Table 4 DSS04 Level 3 Activities

No	Sub Process	Question	Yes/No
1	DSS04.02 Maintain business resilience	Assess the likelihood of threats that could cause loss of business continuity. Identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.	☑
2	DSS04.02 Maintain business resilience	Analyze continuity requirements to identify possible strategic business and technical options.	☑
3	DSS04.02 Maintain business resilience	Identify resource requirements and costs for each strategic technical option and make strategic recommendations.	☑

4	DSS04.02 Maintain business resilience	Obtain executive business approval for selected strategic options.	☑
5	DSS04.03 Develop and implement a business continuity response.	Distribute the plans and supporting documentation securely to appropriately authorized interested parties. Make sure the plans and documentation are accessible under all disaster scenarios.	☑
6	DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).	Schedule exercises and test activities as defined in the continuity plans.	☑
7	DSS04.05 Review, maintain and improve the continuity plans.	On a regular basis, review the continuity plans and capability against any assumptions made and current business operational and strategic objectives.	☑
8	DSS04.05 Review, maintain and improve the continuity plans.	On a regular basis, review the continuity plans to consider the impact of new or major changes to enterprise organization, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.	☑
9	DSS04.05 Review, maintain and improve the continuity plans.	Consider whether a revised business impact assessment may be required, depending on the nature of the change.	☑
10	DSS04.05 Review, maintain and improve the continuity plans.	Recommend changes in policy, plans, procedures, infrastructure, and roles and responsibilities. Communicate them as appropriate for management approval and processing via the IT change management process.	☑
11	DSS04.06 Conduct continuity plan training.	Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.	☑
12	DSS04.06 Conduct continuity plan training.	Develop competencies based on practical training, including participation in exercises and tests.	☑

All questions in the investigation received a "yes" answer, resulting in a 100% score. Given that this surpasses the 85% threshold, the next set of questions should be addressed.

3.16 DSS04 – Manage Continuity Level 4

Table 5 DSS04 Level 4 Activities

No	Sub Process	Question	Yes/No
1	DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).	Conduct a post-exercise debriefing and analysis to consider the achievement.	☑
2	DSS04.06 Conduct continuity plan training.	Based on the exercise and test results, monitor skills and competencies.	☑

3	DSS04.08 Conduct post-resumption review.	Assess adherence to the documented BCP and DRP	☑
4	DSS04.08 Conduct post-resumption review.	Determine the effectiveness of the plans, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organizational structures and relationships.	☑

At this level, all four questions received an affirmative answer, totaling around 100%. The company's responses align with the interview findings.

3.17 DSS04 – Manage Continuity Level 5

Table 6 DSS04 Level 5 Activities

No	Sub Process	Question	Yes/No
1	DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).	Based on the results of the review, develop recommendations for improving the current continuity plans.	☑
2	DSS04.08 Conduct post-resumption review.	Identify weaknesses or omissions in the plans and capabilities and make recommendations for improvement. Obtain management approval for any changes to the plans and apply via the enterprise change control process.	☑

In the final stage at level 5, two questions were asked and received affirmative answers, resulting in a 100% score. However, for objectives APO13 and DSS04, there are differences in outcomes. APO13's questions reached up to level 3 but weren't continued beyond that. In contrast, DSS04 consistently scored above 85% across all levels, suggesting a need for reevaluation until full compliance is attained. The recommendation is to focus on and enhance each aspect of the questions for both objectives to benefit the company.

4. Conclusion

The evaluation of the BPS's IT governance, utilizing the COBIT 2019 framework, reveals both the strengths that the agency possesses and the challenges it needs to address. At the heart of the agency's operations lies a deep commitment to client service and stability, which is evident from the high emphasis placed on the Client Service/Stability section. This focus underscores the agency's dedication to effectively serve the community, ensuring that data and statistical services are readily available and reliable for the public. Delving deeper into specific areas, the assessment highlights the critical importance of EG01, which pertains to the Portfolio of Competitive Products and Services. With a score of 5, it's clear that BPS heavily relies on its diverse publication portfolio as a cornerstone of its service offerings. This reflects the agency's proactive approach in continuously updating and expanding its range of services to meet the evolving needs of its stakeholders. Similarly, EG02, which deals with Managed Business Risk, also scores a 5. This score underscores BPS's commitment to safeguarding its operations against potential risks, particularly in data-centric areas. This commitment is further echoed in areas like EG03 (Compliance with External Laws and Regulations) to EG06 (Business Continuity), where each scores a full 5. These high scores underline the agency's compliance-driven approach, with a clear focus on adhering to legal frameworks, ensuring financial transparency, nurturing a customer-centric culture, and maintaining robust business continuity plans.

However, the BPS’s risk profile paints a somewhat contrasting picture. Notably, IT Operational Infrastructure Incidents and Unauthorized Actions both score a concerning 5. This highlights significant vulnerabilities in the agency's IT infrastructure, pointing to past failures and potential risks from both external and internal sources. Another critical area of concern is Data and Information Management, which also scores a high 5. Given BPS's heavy reliance on accurate and secure data, these scores emphasize the agency's susceptibility to data leaks and the importance of bolstering its data protection measures.

Despite these challenges, BPS's proactive stance towards IT security shines through. The agency assigns a 100% importance rating to IT security in its Compliance Requirements Table. This demonstrates a clear recognition of the crucial role that robust IT security measures play in safeguarding the agency's operations and data assets. To propel its IT governance to new heights, BPS should prioritize enhancing its IT security infrastructure, addressing the vulnerabilities highlighted in its risk profile, and ensuring continuous alignment of its IT strategies with its broader organizational objectives. By doing so, the agency can not only mitigate risks but also optimize its service delivery, fostering greater trust and confidence among its stakeholders.

5. References

[1] P. A. Adawiyah and L. H. Atrinawati, "INFORMATION TECHNOLOGY GOVERNANCE DESIGN USING COBIT 2019 FRAMEWORK AT PT. XYZ,"*J. Technol. And Sis. Inf.*, vol. 1, no. 2, pp. 1–9, Dec. 2020, doi: 10.33365/jtsi.v1i2.301.

[2] A. Intan, A. Setiawan, and M. R. Maengkom, "Literature Study of the Role and Benefits of COBIT 2019 in Information Technology Governance in Indonesia,"*Innov. J.Soc. Sci. Res.*, vol. 3, no. 5, Art. no. 5, Oct. 2023, doi: 10.31004/innovative.v3i5.4966.

[3] G. I. Belo, L. H. Atrinawati, and Y. T. Wiranti, "Designing Information Technology Governance using COBIT 2019 at PT Telekomunikasi Indonesia Regional VI Kalimantan,"*J. Syst. Inf. Dan Ilmu Komput PrimaJUSIKOM PRIMA*, vol. 4, no. 1, Art. no. 1, Sep. 2020, doi: 10.34012/jusikom.v4i1.1202.

[4] "Information Technology Governance Analysis Using The COBIT 2019 Framework at XYZ Institution," E. M. Lompoliu, G. B. R. F. Francolla, G. R. Mandoya, M. D. Walangitan, and J. Y. Mambu.*CogITo Smart J.*, flight. 8, no. 2, Art. no. 2, Dec. 2022, doi: 10.31154/cogito.v8i2.427.346-358.

[5] M. Elazhary, A. Popovič, P. Henrique De Souza Bermejo, and T. Oliveira, "How Information Technology Governance Influences Organizational Agility: The Role of Market Turbulence," *Inf. Syst. Manag.*, vol. 40, no. 2, pp. 148–168, Apr. 2023, doi: 10.1080/10580530.2022.2055813.

[6] A. A. Mariatama, L. H. Atrinawati, and M. G. L. Putra, "INFORMATION TECHNOLOGY GOVERNANCE DESIGN USING COBIT 2019 FRAMEWORK AT PT JWT GLOBAL LOGISTICS INDONESIA,"*J. Syst. Inf. Law Information. Simika*, vol. 5, no. 1, Art. no. 1, Feb. 2022, doi: 10.47080/simika.v5i1.1423.

[7] S. Haes, W. Grembergen, A. Joshi, and T. Huygh, "COBIT as a Framework for Enterprise Governance of IT," 2020, pp. 125–162. doi: 10.1007/978-3-030-25918-1_5.

[8] arief, "CobIT (Control Objectives for Information Technology)," ITGID | IT Governance Indonesia. Accessed: Oct. 31, 2023. [Online]. Available: https://itgid.org/cobit-control-objectives-for-information-technology/

[9] P. N. Anastasia and L. H. Atrinawati, "INFORMATION TECHNOLOGY GOVERNANCE DESIGN USING COBIT 2019 FRAMEWORK AT HOTEL XYZ,"*JSI J. Sist. Inf. E-J.*, vol. 12, no. 2, Oct. 2020, doi: 10.36706/jsi.v12i2.12329.

[10] J. D. S. 6-8 10710 J. I. S. map: G. Maps, "Badan Pusat Statistik (BPS - Statistics Indonesia)." Accessed: Oct. 31, 2023. [Online]. Available: https://landportal.org/node/92471

[11] A. F. Wijaya, "Analysis and Design of Information Technology Governance Using the COBIT 2019 Framework at PT. XYZ,"*J. Comput. Inf. Syst. Ampera*, Jan. 2022, Accessed: Oct. 31, 2023. [Online]. Available:

https://www.academia.edu/84400768/Analisis_dan_Desain_Tata_Kelola_Teknologi_Informasi_Menggunakan_Framework_COBIT_2019_pada_PT_XYZ