JDBIM
(Journal of Digital Business and Innovation Management)

Volume 4 No.2, December 2025, 378-392
ISSN 2962-3898 (Online)
DOI: 10.26740/jdbim.v4i2.71778
https://ejournal.unesa.ac.id/index.php/jdbmi/index

Development of Audit Working Papers and Maturity Levels for Helpdesk Information Technology Governance Using COBIT 2019 in the DSS Domain: (A Case Study of XYZ University)

Syifa'ul Aini Zahroh[1]*, Renny Sari Dewi[1], Rindu Puspita Wibawa[2]

[1] Department of Digital Business, Faculty of Economics and Business, Universitas Negeri Surabaya, Jalan Ketintang, Surabaya 60231, Indonesia [2] Directorate of Cooperation, Information Technology and Data Center,
Universitas Negeri Surabaya, Jalan Lidah Wetan, Surabaya 60213, Indonesia

syifaulaini.21020@mhs.unesa.ac.id

Abstract

The implementation of the helpdesk information system at University XZY in Surabaya plays a crucial role in supporting the management of complaints from students and academic staff. However, several issues have been identified, including inadequate user data verification mechanisms, potential privacy violations due to open access to complaint reports by other users, and the absence of a structured incident resolution report. These challenges impact the performance and integrity of the information system. To address these problems, this study aims to design an audit working paper using the COBIT 2019 framework, specifically focusing on DSS02 (Managed Service Requests and Incidents), DSS03 (Managed Problems), and DSS04 (Managed Continuity) to evaluate and improve the system. The findings indicate that all three domains are at capability level 3 (Defined), which implies that processes are documented but not yet measured consistently. This study produces an audit working paper, improvement recommendations, and an implementation cost estimation, which can serve as a strategic reference for university XYZ in enhancing the quality, security, and sustainability of its helpdesk system.

Keywords: Information system audit; COBIT 2019; Audit Working paper; Helpdesk; DSS

Received: 1 June 2025; Accepted: 25 July 2025; Published: December 2025

To cite this document:
Zahroh, S. A., Dewi, R. S., & Wibawa, R. P. (2025). Development of Audit Working Papers and Maturity Levels for Helpdesk Information Technology Governance Using COBIT 2019 in the DSS Domain: (A Case Study of XYZ University). *JDBIM (Journal of Digital Business and Innovation Management)*, Vol. 4 Np. 2, pp. 378-392. DOI link

*Corresponding author
Email: syifaulaini.21020@mhs.unesa.ac.id

Abstrak

Implementasi sistem informasi helpdesk diperguruan tinggi XYZ di Surabaya memiliki peran dalam membantu pengelolaan pengaduan mahasiswa dan tenaga kependidikan. Namun, terdapat permasalahan antara lain mekanisme verifikasi data pengguna yang belum memadai, pelanggaran privasi karena pengaduan dapat dilihat oleh pengguna lain dan tidak adanya laporan penyelesaian insiden yang terstruktur. Tantangan tersebut memiliki dampak pada sistem informasi, untuk menangani permasalahan tersebut penelitian ini bertujuan untuk melakukan perancangan kertas kerja menggunakan kerangka kerja COBIT 2019 khususnya DSS02 (Managed Service Requests and Incidents), DSS03 (Managed Problems), dan DSS04 (Managed Continuity) dalam mengevaluasi dan memperbaiki sistem. Hasil temuan dari ketiga domain berada pada level 3 (defined) menunjukkan sistem sudah berjalan namun belum terukur secara berkelanjutan. Penelitian ini menghasilkan kertas kerja audit dan rekomendasi perbaikan serta estimasi biaya implementasi yang dapat digunakan sebagai pertimbangan strategis bagi perguruan tinggi XYZ di Surabaya dalam meningkatkan kualitas, keamanan, dan keberlanjutan layanan.

***Kata kunci**: Audit sistem informasi; COBIT 2019; kertas Kerja Pemeriksaan; Layanan Pengaduan; DSS*

INTRODUCTION

Universities, engaged in digital transformation, have a responsibility to provide responsive, efficient, and transparent academic and administrative services. The development of a helpdesk information system to maintain the quality of information technology governance provides a means for students and educational staff to submit complaints and incidents related to academic and non-academic services (Amrulloh et al., 2020). The implementation of a helpdesk information system managed by the Information Technology Development Center at XYZ University in Surabaya revealed various weaknesses, such as the lack of integrated verification through Single Sign-On, weak privacy protection for user data reports, and the lack of automated incident report resolution, all of which have the potential to weaken service governance and impact the quality and trust of users.

The implementation of the helpdesk information system has been shown to not fully guarantee aspects of security, privacy, and operational effectiveness. Risks such as weak oversight of service requests, misuse of access, and delays in incident resolution create serious challenges to the sustainability of digital services (Ivander & Papilaya, 2023; Ramadhan et al., 2020). Information system audits can be used to identify weak points for risk

management and evaluate the accuracy of internal controls, reliability and security of information systems used to support academic activities (Destriani & Putra, 2023).

Previous research proves that the use of the 2019 COBIT framework is effective in managing helpdesk information systems in the higher education environment. Safitri et al (2023) implementing COBIT 2019 can provide a performance assessment to find areas that need to be improved, especially the DSS subdomain. while Arifa et al. (2023) also used COBIT 2019 which had a positive impact on increasing system responsiveness in meeting user needs and maintaining the security of processed data.

In this study, the COBIT 2019 framework was chosen as the primary approach, providing a structure for IT strategies, processes, and activities to measure more effective and optimal levels of governance capabilities, particularly in the Delivery, Service, and Support domain (Arifa et al., 2023). The Delivery, Service, and Support (DSS) domain has subdomains such as DSS02 (Managed Service Requests and Incidents), which focuses on managing incidents and service requests; DSS03 (Managed Problems), which addresses the root cause of problems to prevent recurrence; and DSS04 (Managed Continuity), which ensures incident and complaint handling is carried out according to standards (Safitri et al., 2023). Using this approach, the helpdesk information system is expected to reach maturity using the CMMI model implemented in COBIT 2019 (Akbar et al., 2025).

Based on the identified problems and opportunities, this study aims to design a COBIT-based information system audit worksheet as an instrument to evaluate the effectiveness of controls and processes in the helpdesk information system of XYZ University in Surabaya. To generate recommendations for corrective improvements (Nugraha, 2020). The development of an information system audit worksheet based on COBIT

2019 provides guidance to assist universities in conducting continuous audits so that they can identify and follow up on areas that need improvement to improve the performance of the university's operational system (Destriani & Putra, 2023).

LITERATURE REVIEW

Information System Audit

Information system audit is a systematic evaluation process to assess the effectiveness and achievement of organizational goals through auditor evidence to assess performance in aspects of internal control, security and operational efficiency, especially in a digitized higher education environment (Purwaningrum et al., 2021). Through information system audits ensure data protection, increase stakeholder confidence through national and international compliance standards (Fakeyede et al., 2023). The purpose of information system audits is in line with the security principles of Confidentiality, Integrity and Availability (CIA Triad) which protect information from unauthorized access, manipulation and service disruption (Thenu & Rudianto, 2024; Yee & Zolkipli, 2021). By applying the CIA principle, organizations can build a robust information security system in supporting data-based decision making, minimizing the risk of disruption while increasing compliance with policies in system management (Al Morizha et al., 2025; Sirait & Nasution, 2024).

Framework COBIT 2019

Control Objectives for Information and Related Technologies (COBIT) 2019 is a governance and information management framework developed by ISACA to assist organizations in managing and directing IT effectively (Saleh et al., 2021). COBIT divides governance into two areas, namely Governance which ensures IT is aligned with the vision and goals of the organization and Management which focuses on managing IT services operationally to be efficient and responsive to business needs (ISACA, 2018). In the study of helpdesk information systems, it focuses on the Deliver, Service and Support (DSS) domain which helps organizations, especially universities, maintain information security, increase user confidence and ensure that the helpdesk system provides added value

JDBIM (Journal of Digital Business and Innovation Management)
Volume 4 No.2, December 2025
E-ISSN 2962-3898
Page 378-392

through reliable and sustainable IT management (Dewi et al., 2024; Tulung et al., 2023). COBIT 2019 supports CMMI-based capability measurement to assess the organization's maturity level and ability to manage risk and improve service quality. (Indrawati et al., 2023).

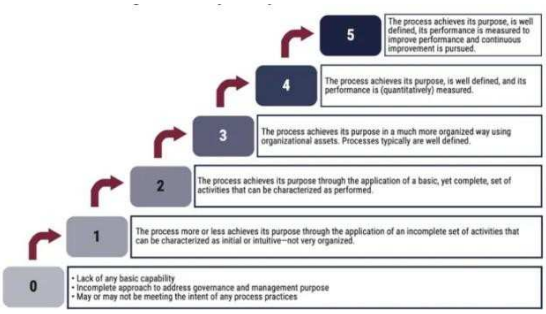

Figure 1 Capability Level for Processes

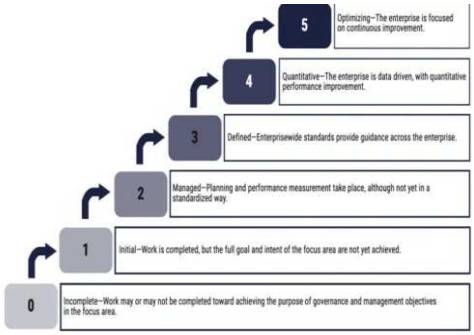

Figure 2 Maturity Level for Focus Area

At the Capability Level stage, measurements are focused on assessing the extent to which a process supports information technology specifically and objectively, thereby helping organizations identify weaknesses and opportunities for improvement to achieve desired results (Akbar & Panjaitan, 2025). Meanwhile, within the COBIT 2019 framework, Maturity Level measurements serve as a comprehensive performance evaluation tool at the focus area level, providing a broader view than capability level alone (Akbar, 2024). Maturity level also reflects the level of implementation, management, and continuous improvement carried out by an organization in accordance with standards and best practices, thus helping organizations understand their current maturity level and formulate strategic steps to improve IT governance (D. A. Kurniawan et al., 2024).

METHODS

The research uses a qualitative approach to analyze and explore more deeply the condition of the implementation of the helpdesk information system at XYZ Surabaya college, especially the Domain, Deliver Service annd Support (DSS) domain in the COBIT 2019 framework. The research focus includes analyzing internal policies, technical procedures and information control security. The research approach can explore holistically to influence the effectiveness and reliability of the incident handling process, service requests and user data protection.

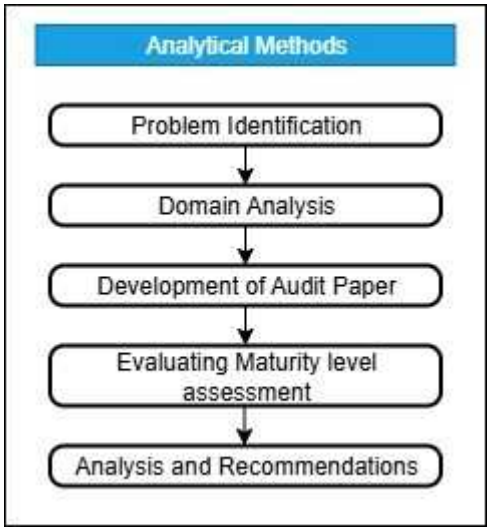

Figure 3 Analytical Methodology

Figure 3 s Figure 3 shows the Analysis Methodology, which is a research flow using a qualitative approach in a case study. The identification of problems is preceded by the collection of data. This data is gathered through observation and in-depth interviews with technical staff from the information technology development team. Next, the domain analysis stage uses the toolkit provided by ISACA. The toolkit is mapped to obtain domain results that align with the organization's business process requirements. This alignment facilitates the deepening of the implementation process with the COBIT 2019 standard.

The audit working paper design stage includes the following: identifying problems, documenting evidence, evaluating controls, and making improvement recommendations. These recommendations are based on a capability assessment using the Capability Maturity Model Integration model, which ranges from level 0 to level 5. The audit evaluation stage is conducted to obtain valid and comprehensive data identifying factors affecting the effectiveness of the help desk system in accordance with the COBIT 2019 standard and information security principles, such as CIA.

The COBIT 2019 standard serves as a reference in providing a structure for preparing audit workpapers integrated with organizational needs within the DSS framework to enhance data security and standards compliance, reflecting the organization's actual conditions. This approach yields findings that describe the current system condition and provide recommendations for improving the quality of information technology- based services.

JDBIM (Journal of Digital Business and Innovation Management)
Volume 4 No.2, December 2025
E-ISSN 2962-3898
Page 378-392

RESULT AND DISCUSSION

1. Problem Identification

The helpdesk information system of XYZ university in Surabaya shows problems that affect service quality, related to the absence of an identity verification mechanism, every user data reporting can be seen by everyone and the absence of automation in closing incidents. These incidents show gaps in the helpdesk system that allow responsible parties to threaten privacy in identity theft and reduce trust and reputation of the institution. These problems emphasize the importance of evaluating and improving the system using the COBIT 2019 framework which is able to identify weaknesses and provide systematic guidance in improving service reliability and security so as to support user confidence through designing audit work papers as needed.

2. Domain Analysis

COBIT 2019 has a design toolkit for mapping which includes 10 design factors as a reference basis for determining subdomains. Based on the identification of the needs of XYZ Surabaya University, it produces an overview of the relationship between the strategic needs of the organization and the COBIT 2019 domain, especially the DSS domain as a basis for preparing audits and improving an effective and structured helpdesk system (Indrawati et al., 2023). The mapping results can be seen in Figure 4.

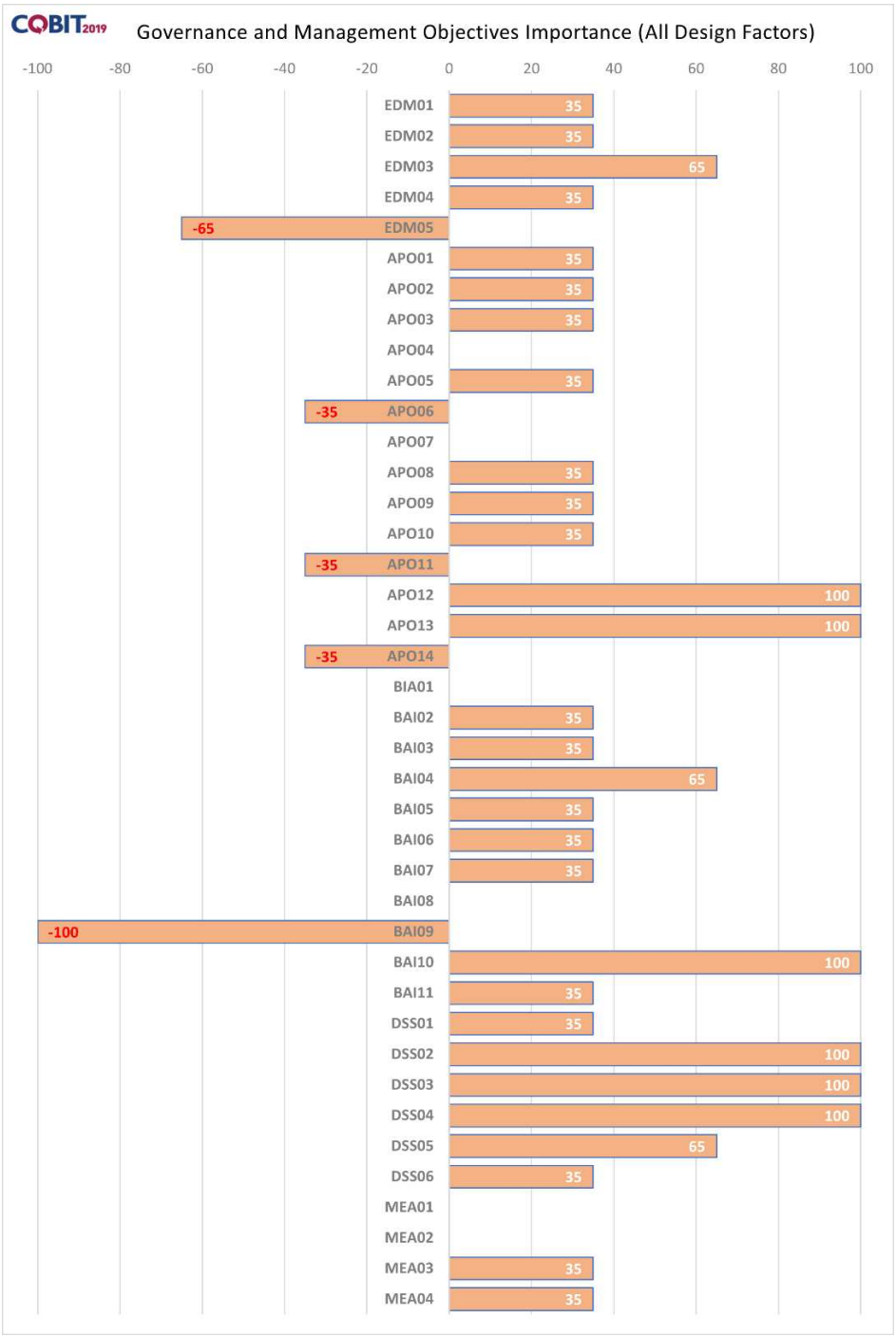

Figure 4 Design Factors

The selection of subdomains in COBIT 2019 is not mandatory based on the results but can be chosen based on the organization's needs to improve governance and management areas. Based on the results of the design factor mapping with a research focus using design factors, it

JDBIM (Journal of Digital Business and Innovation Management)
Volume 4 No.2, December 2025
E-ISSN 2962-3898
Page 378-392

shows that the subdomains DSS02, DSS03 and DSS04 have alignment in managing issues related to data verification and protection as well as automation of incident resolution for the helpdesk system which can operate when disruptions occur in maintaining service stability.

3. Development of Audit Paper

The audit instruments are systematically developed in accordance with the COBIT 2019 framework practice standards, specifically for the Deliver, Service, and Support domain, which focuses on DSS02, DSS03, and DSS04. The audit instruments consist of process audit instruments, checklist audit instruments, and step audit instruments for each subdomain process, covering the procedural, technical, and documentation aspects of each service process. The instruments were developed with reference to the organization's needs to support operational activities in achieving the indicators set by COBIT 2019.

Based on the preparation of information system audit working papers for each subdomain, they are used to ensure the effectiveness of IT service and support management within the organization. The DSS02 (Managed Service Request and Incidents) subdomain consists of 33 audit instrument documents aimed at evaluating and ensuring the systematic and documented handling of service requests to minimize disruption to IT services. The DSS03 (Managed Problems) subdomain consists of 28 audit instrument documents focused on identifying root causes and preventing recurrent incidents, which impacts service quality and stability. DSS04 (Managed Continuity) consists of 53 audit instrument documents aimed at assessing an organization's readiness to maintain the continuity of IT services through planning, testing, and maintaining a sustainable risk management strategy in accordance with COBIT 2019 principles.

4. Evaluating Maturity Level Assessment

The process maturity level assessment in the 2019 COBIT framework is a strategic step to identify the implementation of effectiveness in the XYZ Surabaya college helpdesk system. The assessment was carried out using a scale of 1-5 according to the COBIT 2019 Govarnance and Management Objectives guide (ISACA, 2019) The results of research that focuses on three DSS subdomains DSS02 (Managed Service Requests and Incidents), DSS03 (Managed Problems), and DSS04 (Managed Continuity), show scores that support system improvements

with the aim of supporting system improvements that are aligned with business goals and stakeholder expectations detailed in table 1 maturity level.

Table 1 Maturity Level

Domain	Proces	Score
DSS02	Manage Service Requests and Incidents	2,6
DSS03	Manage Problems	2,75
DSS04	Manage Continuity	3
Nilai Rata-Rata		2,8

From the assessment results in Table 1, the DSS02 subdomain (Managed Service Requests and Incidents) showed a score of 2.6, namely (Managed to Defined), as described in Figure 2, previously, in the DSS02 subdomain, it was found that incident classification had not been carried out systematically. Service requests and incidents were handled using an ad hoc approach, without standard guidelines. The procedures for reporting incidents are not documented well, and the ticketing system does not have an automatic closure mechanism. Additionally, management cannot use the periodic incident trend reporting for predictive analysis.

The subdomain DSS03 (Managed Problems) scored 2.75 (Managed to Defined), indicating that there is no structured mechanism for recording known errors. The organization also does not investigate the root causes of recurring incidents. Consequently, the same incidents are likely to recur without long-term mitigation. Periodic evaluations of the effectiveness of problem resolution have also not been conducted.

The evaluation of sub-domain DSS04 (Managed Continuity) reveals a score of 3 (Define), suggesting that the organization has initiated measures to ensure service continuity. However, a more thorough evaluation of the entire DSS04 domain reveals several areas in need of significant improvement. Currently, the organization lacks a formally documented business continuity plan (BCP) and disaster recovery plan (DRP). The absence of these critical documents hinders the organization's ability to respond to major incidents in a structured and effective manner.

Additionally, regular system recovery simulations or tests have not been conducted. These routine tests are crucial for verifying the effectiveness of recovery procedures and identifying potential weaknesses before a real incident occurs. Furthermore, personnel responsible for service continuity have not received training in the knowledge and skills required to manage crises, minimize impact, and

JDBIM (Journal of Digital Business and Innovation Management)
Volume 4 No.2, December 2025
E-ISSN 2962-3898
Page 378-392

quickly restore services.

Based on Table 1, the results of the maturity level in each subdomain are visualized to show the performance of each subprocess so that it helps identify patterns of inequality between processes to facilitate analysis of areas that require priority improvement.

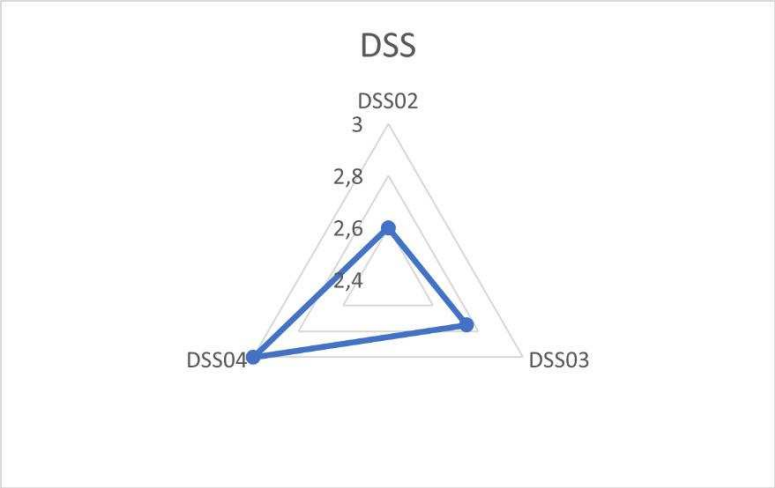

Figure 5 Radar Chart DSS

Based on Figure 5, the summary visualization of the capability levels of the three subdomains shows an imbalance in the priority areas for improvement. Therefore, the organization needs to strengthen formal documentation, build measurable performance indicators, and automate service processes. With this approach, the retirement information system can run efficiently, responsively and in line with IT governance objectives.

5. Analysis and Recommendation

The implementation of the helpdesk information system evaluation at XYZ college aims to measure the level of operational management during incidents in handling service continuity in accordance with the COBIT 2019 standard. Several weaknesses were found that have the potential to affect the quality to users. These findings provide a basis for recommendations for improvements to information systems by considering cost estimates in strategic planning and resource allocation that are aligned with the 2019 COBIT value and performance principles tailored to the needs of XYZ college. Then the following cost estimates for each subdomain

- Rekomendasi DSS02

  Evaluation of the helpdesk information system at XYZ college using the COBIT 2019 framework identifies weaknesses that have the potential to affect service quality and user satisfaction, and provides targeted improvement recommendations based on these

findings. In addition to technical aspects, the evaluation also considers the estimated costs required to support the college's strategic planning and resource allocation, following the implementation details of the category component.

Table 2 Cost Estimate DSS02

Category	Key Componen
Self-service Features	AI chatbot, automated reporting, notification
Security Systems	SIEM, multifactor authentication, RBAC
Supporting Infrastructure	Storage, incident repository, audit trail
Process Automation	Workflow automation, incident tracking
IT internal training	IT team training

From table 2, the total estimated cost for all DSS02 recommendations ranges from Rp. 120,900,000 to Rp. 318,500,000, depending on the scale of implementation and adjustment to the specific needs of the organization. This investment covers both technical and non-technical aspects to build a secure, efficient, and sustainable system according to the principles of good IT governance.

- Recommendation DSS03

Evaluation of the maturity level of the 2019 COBIT framework on the helpdesk system identifies crisis weaknesses in incident management and problems that have an impact on service quality. In table 3 the recommendations for key component DSS03.

Table 3 Cost Estimate DSS03

Category	Key Component
Incident Identification	Automated log analysis, real-time notifications
Impact monitoring	Continuous monitoring system, CI documentation
Change Management	SOP development, risk assessment procedures, team training
Post incident analysis	Root cause analysis, automated user notifications, feedback tracking
Problem Manaagement	RCA systems, temporary solutions, SLA evaluation dashboards, access audits

The DSS03 implementation, with an estimated budget of IDR 55–141.5 million, represents a strategic investment to enhance incident and problem management through automated identification, real-time monitoring, and root cause analysis. Prioritizing core systems

JDBIM (Journal of Digital Business and Innovation Management)
Volume 4 No.2, December 2025
E-ISSN 2962-3898
Page 378-392

like impact monitoring and RCA implementation will yield the highest operational returns, including 30–40% faster incident resolution and 25% fewer recurring issues. Cost optimization can be achieved through phased deployment, open-source solutions, and bundled vendor contracts, while a 10–15% contingency should be allocated for integration and training needs. This transformation from reactive to proactive incident management will significantly improve SLA compliance (15–20%) and service reliability, making it essential to align implementation with fiscal planning and vendor selection for long-term sustainability.

- Recommendation DSS04

  Implementation in DSS04 helpdesk system to strengthen incident management and service continuity then each component is structured to support a fast, accurate response to service disruptions and ensure continuous improvement according to the needs of the college. The following are the details and components in table 5

Category	Key Component
BCM Policy development	BCM framework, RTO/RPO policies, PDP Act compliance
Disaster Preparedness	BIA analysis, monitoring tools, BCP/DRP documentation
Backup Infrastructure	Automated backup systems, redundant storage, recovery testing
BCM Training	Technical drills, CAB team formation, certification programs
Resilience Audit	BCP-DRP simulation, compliance auditing, improvement reports

The DSS04 COBIT 2019 domain-based implementation at XYZ University is estimated to require a budget of between IDR 218.7 million and IDR 425.5 million. The primary focus is on strengthening disaster preparedness and backup infrastructure, which accounts for approximately 60% of the total cost. Efficiency strategies include leveraging existing IT infrastructure, tiered storage, and phased procurement. Expected benefits include up to an 80% reduction in data loss, 50% improved system recovery efficiency, and annual compliance savings of up to IDR 60 million.

CONCLUSION

The application of the COBIT 2019 framework, especially in domains DSS02, DSS03, and DSS04, provides a systematic approach in evaluating and improving the quality of digital-based complaint service information systems. Evaluation of the DSS02 domain shows that the process of handling service requests and incidents is already running, but it is not yet fully documented properly, which has the potential to cause inconsistencies and errors in reporting. In the DSS03 domain, strengthening is still needed in root cause documentation, error discovery, and risk management to prevent recurring incidents. Meanwhile, the DSS04 domain indicates that service continuity has been considered but has not been supported by formal documents and sufficient training to ensure preparedness in the face of operational disruptions. Strengthening the helpdesk system requires the development of formal procedures, improved automation systems, and ongoing internal training. Technology integration such as multifactor authentication, automated notification systems, and dashboard monitoring will improve security, responsiveness, and service efficiency. In addition, the development of SOPs, recovery simulations, and periodic audits are necessary to ensure operational continuity and overall data protection. This approach will build a strong foundation for an adaptive, secure, and sustainable digital service system according to modern information technology governance standards.

REFERENCES

Akbar, M. D. A., & Panjaitan, E. S. (2025). Evaluasi Tatakelola TI Menggunakan Framework COBIT 2019 dan Capability Maturity Model Integration (CMMI). Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi), 9(2), 765–775.

Amri, A. (2015). Manajemen risiko-ISO 31000. *ITB BLOGS*, *15*.

Amrulloh, A., Wibisono, G., Mido, A. R., & others. (2020a). Audit Tata Kelola Teknologi Informasi Pada Perguruan Tinggi Menggunakan Cobit 5 Fokus Proses Pelayanan: Array. *Jurnal Ilmiah KOMPUTASI*, *19*(1), 115–120.

Arifa, S., Isnanto, R., & Kridalukmana, R. (t.t.-a). Analysis Of University Helpdesk Information Technology Governance Using Cobit 2019 And Fuzzy Ahp. *Jurnal Teknologi Informasi Universitas Lambung Mangkurat (JTIULM)*, *8*(2), 31–40.

Astuti, H. M., Muqtadiroh, F. A., Darmaningrat, E. W. T., & Putri, C. U. (2017). Risks assessment of information technology processes based on COBIT 5 framework: A case study of ITS service desk. *Procedia Computer Science*, *124*, 569–576.

Destriani, M., & Putra, Y. H. (2023). Rencana Audit Tata Kelola Sistem Informasi Di Universitas Subang Menggunakan Framework COBIT 2019. *Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi*, *9*(1), 19–33.

Desy, I., Hidayanto, B. C., & Astuti, H. M. (2014). Penilaian risiko keamanan informasi menggunakan metode failure mode and effects analysis di divisi TI PT. Bank XYZ Surabaya. *SESINDO 2014*, *2014*.

Hanif, D. A., & Suryaningrum, D. H. (2024). Analisis Prosedur Kertas Kerja Audit Beban Pada Pt. Dealer Mercedes Benz Oleh Kap Kps. *Jurnal Revenue: Jurnal Ilmiah Akuntansi*, *5*(1), 771–778.

Indrawati, A. R., Rozas, I. S., & Wahyudi, N. (2023). Penyusunan Instrumen Maturity Assessment Design Toolkit Berbasis COBIT 2019. *Edu Komputika Journal*, *10*(1), 64–71.

Ivander, D. L., & Papilaya, F. S. (2023). Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000: 2018. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *4*(2), 1042–1051.

ISACA. (2018). COBIT® 2019: Designing an Information and Technology Governance Solution.

Khairunnisa, P., Nasution, N. S., Nirwana, I., & Megawati, M. (2024b). Evaluasi Tingkat Capability Sistem Informasi Akademik Menggunakan Framework Cobit 2019 Di Perguruan Tinggi Xyz. *Scientica: Jurnal Ilmiah Sains dan Teknologi*, *2*(8), 14–20.

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, *125*, 691–697.

Nugraha, M. B. (2020). *Penyusunan Instrumentasi Tata Kelola & Audit Pelayanan Jaringan Komputer Di Lingkup Pemerintah Kabupaten Gresik Menggunakan Framework Cobit 4.1* (Doctoral dissertation, Universitas Internasional Semen Indonesia).

Ramadhan, D. L., Febriansyah, R., & Dewi, R. S. (2020). Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ. *JURIKOM (Jurnal Ris. Komputer)*, *7*(1), 91.

Safitri, R. A., Mutiah, N., & Febriyanto, F. (2023). Information technology services management audit using the cobit and itil framework. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, *9*(2), 231–238.

Saleh, M., Yusuf, I., & Sujaini, H. (2021). Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas. *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, *7*(2), 204–209.