ARTICLE

Enhancing Information Technology Governance at the University of Riau Library

A Capability Analysis Using the COBIT 5 Framework

Yanti Andriyani, Evfi Mahdiyah, Agung Santoso, and Riki Ario Nugroho

ABSTRACT

Effective information technology (IT) governance is essential for the University of Riau (UNRI) Library to achieve its research and educational objectives. This paper presents a qualitative pilot study investigating the library's current IT governance processes, focusing on two COBIT 5 processes—DSS01 (Manage Operations) and DSS05 (Manage Security Services). These processes were selected in consultation with library and IT leadership due to their direct relevance to ensuring operational reliability and safeguarding the library's information assets. COBIT 5 principles and capability models guide the assessment, emphasizing regulatory compliance, performance monitoring, and stakeholder collaboration. Using a detailed questionnaire and capability model, the study evaluates base practices and work products for DSS01 and DSS05. Results indicate varying proficiency levels, with DSS01 at level 0 and DSS05 at level 1, highlighting significant gaps between current and desired capability levels. Recommendations include implementing standard operating procedures, enhancing security measures, and optimizing resource management. In conclusion, the findings underscore the need for standardized processes, continuous monitoring, and alignment with established frameworks like COBIT 5. By addressing identified gaps and implementing recommended improvements, the UNRI Library can strengthen its IT governance, enhance operational efficiency, and better support its academic mission.

INTRODUCTION

Effective information technology (IT) governance is crucial for the University of Riau (UNRI) Library to achieve its research and educational objectives, particularly within the library, which serves as a critical hub for academic resources and services.[1] The library's reliance on integrated IT systems—including cataloguing platforms, circulation systems, academic work repositories, and publication management tools—means that its performance directly affects the quality and accessibility of information for students, faculty, and researchers.

The UNRI Library operates within a centralized IT governance model, where infrastructure provisioning, enterprise-wide security policies, and major technology investments are coordinated by the university's central IT office. This arrangement ensures consistency across campus systems but can also limit the library's autonomy in adopting governance frameworks such as COBIT 5. The library retains operational control over certain functions—such as managing its local applications, defining service workflows, and overseeing some security measures—but any governance practices must align with overarching institutional policies.[2] This shared

About the Authors

Yanti Andriyani (yanti.andriyani@lecturer.unri.ac.id; corresponding author) is Assistant Professor, University of Riau. **Evfi Mahdiyah** (evfi.mahdiyah@lecturer.unri.ac.id) is Assistant Professor, University of Riau. **Agung Santoso** (agung.santoso@student.unri.ac.id) is Bachelor's Student, University of Riau. **Riki Ario Nugroho** (riki.ario@lecturer.unri.ac.id) is Assistant Professor, University of Riau.

Submitted: 10 May 2025. Accepted for Publication: 6 December 2025. Published: 15 June 2026.

https://doi.org/10.5860/ital.v45i2.17436

authority requires that the adoption of COBIT 5 processes be carefully coordinated to complement, rather than conflict with, the central IT office's chosen governance approach.

Managing these systems effectively presents persistent challenges. The library operates under a centralized institutional IT structure, which ensures policy consistency but can limit autonomy in decision-making.[3] Budget constraints, rapidly evolving technology landscapes, cybersecurity threats, and the diverse needs of library users further complicate operational management.[4] These factors increase the risk of service disruptions, security breaches, and inefficiencies that can undermine the library's mission.[5]

Given these challenges, adopting a structured IT governance approach is advisable to align technology initiatives with institutional goals, strengthen accountability, standardize procedures, and support continuous performance monitoring. In this study, COBIT 5 was used as the guiding framework to assess two priority processes: DSS01 (Manage Operations) and DSS05 (Manage Security Services).

Our study aims to identify improvement strategies for the UNRI Library by demonstrating how enhancing IT efficiency through robust governance practices can elevate its strategic positioning, foster innovation, and enhance overall performance. By investing in IT governance and leveraging frameworks like COBIT, the UNRI Library can address challenges, strengthen its position as a leading academic institution, and provide exceptional services to its users, thereby fulfilling its mission more effectively.

RELATED LITERATURE

COBIT 5

COBIT 5 (Control Objectives for Information and Related Technologies version 5) is a globally recognized framework developed by the Information Systems Audit and Control Association (ISACA) for governing and managing enterprise IT.[6] Organizations can use this extensive set of standards, procedures, and principles to govern and manage information and technology resources efficiently and to support the achievement of strategic goals.

COBIT 5 is structured around five key principles:[7]

1. Meeting Stakeholder Needs: Organizations must align their IT initiatives with the needs and expectations of stakeholders, including customers, shareholders, regulators, and employees.
2. Integrating Every Aspect of the Enterprise: COBIT 5 highlights the significance of managing IT in an integrated manner from operational execution to strategic planning.
3. Applying a Single Integrated Framework: Instead of relying on multiple disparate frameworks, COBIT 5 offers a unified approach to IT governance and management, facilitating consistency and integration.
4. Enabling a Holistic Approach: COBIT 5 encourages organizations to consider various aspects of IT governance, including processes, organizational structures, culture, and enabling technologies.
5. Separating Governance from Management: COBIT 5 distinguishes between governance (setting objectives, evaluating performance, and providing oversight) and management (planning, building, running, and monitoring activities), ensuring clear accountability and decision-making.[8]

COBIT 5 defines five domains for effective IT governance:

1. Evaluate, Direct, and Monitor: Establishes governance frameworks, defines strategic objectives, and monitors alignment with goals.
2. Align, Plan, and Organise: Focuses on planning IT assets, risk management, and optimizing IT investments.
3. Build, Acquire, and Implement: Covers project management, systems development, and change management.
4. Deliver, Service, and Support: Manages service desk operations, incident management, and service levels.
5. Monitor, Evaluate, and Assess: Monitors IT performance, assesses risks, and supports decision-making based on feedback.

To effectively manage and govern these domains, organizations can use a capability model consisting of six levels to assess how well processes are implemented.[9] At level 0, processes are incomplete and lack control and consistency. Level 1 indicates that processes are performed but may be ad-hoc and inconsistent, with limited control and documentation. At level 2, processes are managed and documented with some control and consistency but still need improvement for full effectiveness. Level 3 represents well-established processes that are consistently applied and documented, with defined control and regular performance monitoring. Level 4 shows that processes are optimized for efficiency and effectiveness, with predictable performance and a proactive approach to continuous improvement. Finally, level 5 indicates that processes are continually monitored, refined, and optimized to meet changing business needs, fostering a culture of innovation and excellence.

To determine the effectiveness of these processes, measurements were conducted at each level by analyzing base practices and work products using a detailed questionnaire for each subdomain area. The data collected from these questionnaires were processed to determine the capability levels based on the NPLF scale. In this paper, *NPLF* refers to the four-point achievement rating used in ISO/IEC process assessment: N = not achieved, P = partially achieved, L = largely achieved, and F = fully achieved.[10] This terminology and its typical threshold interpretation (0–15%, >15–50%, >50–85%, >85–100%) originate from the ISO/IEC 15504 process assessment standard and are widely used in process capability assessments, including COBIT 5 process capability assessment approaches.[11] This scale categorizes achievement levels as the following: not achieved (0–15% achievement), indicating minimal achievement of process attributes; partially achieved (>15–50% achievement), showing some attributes are met but with many aspects still unpredictable; largely achieved (>50–85% achievement), indicating significant effort and achievement despite some weaknesses; and fully achieved (>85–100% achievement), demonstrating complete and systematic efforts with no significant weaknesses.

Relevance of COBIT 5 to University Library Governance

University libraries depend heavily on information technology to deliver essential services such as digital cataloguing, circulation management, access to electronic journals, and the preservation of academic outputs. Any breakdown in these systems can significantly disrupt teaching, learning, and research activities.[12] As the complexity of IT infrastructures grows, so does the need for governance frameworks that ensure stability, security, and alignment with institutional priorities.

COBIT 5 provides a structured and measurable approach for assessing and improving IT governance capabilities.[13] Its process-oriented methodology enables libraries to identify gaps,

standardize procedures, and implement controls that directly support their strategic objectives. For example, the DSS01 (Manage Operations) process can help formalize routine maintenance schedules, track infrastructure performance, and improve system uptime, while DSS05 (Manage Security Services) supports proactive threat detection, access control, and compliance with data protection regulations.[14]

Practical applications in similar contexts illustrate the framework's relevance. The universities in Gauteng province, South Africa applied COBIT-based assessments to streamline their server maintenance protocols, resulting in reduced downtime and faster recovery from technical failures.[15] Iran Public Libraries Foundation used COBIT's security management processes to strengthen multi-factor authentication for remote access to e-resources, significantly decreasing unauthorized access incidents.[16] These examples demonstrate how targeted use of COBIT 5 processes can directly enhance operational reliability and safeguard digital assets in an academic library setting.

ANALYSIS PROCESSES

The IT governance assessment at the UNRI Library utilizes the COBIT 5 framework to analyze and measure process capability levels, with a specific focus on the DSS01 (Manage Operations) and DSS05 (Manage Security Services) processes. This assessment is pivotal for gaining insights into the current state of IT governance and pinpointing areas for enhancement.

The DSS01 process aims to ensure that IT operational services are carried out as planned. This process includes five subprocesses:

1. DSS01.1: Perform IT operational procedures
2. DSS01.2: Manage outsourced IT services
3. DSS01.3: Monitor IT infrastructure
4. DSS01.4: Manage the IT environment
5. DSS01.5: Manage facilities

Each subprocess is evaluated to determine how effectively the library manages its IT operations, ensuring they are performed efficiently and reliably.

The DSS05 process focuses on managing security services to protect the IT environment from various threats. It comprises seven subprocesses:

1. DSS05.1: Protect against malware
2. DSS05.2: Manage network and connectivity security
3. DSS05.3: Manage endpoint security
4. DSS05.4: Manage user identity and logical access
5. DSS05.5: Manage physical access to IT assets
6. DSS05.6: Manage sensitive documents and output devices
7. DSS05.7: Monitor infrastructure for security-related events

Evaluating these subprocesses helps ensure that the library's IT services are secure and that sensitive information is protected.

The initial phase of the assessment process for this research adopted a structured approach, commencing with the collection and review of supporting documents such as the library profile, vision, mission, objectives, and organizational structure of the UNRI Library. The library profile

provided essential insights into the organizational framework, laying the groundwork for subsequent actions. The vision, mission, and goals of the organization served as guiding principles, helping to delineate the specific research area and foster a focused approach toward achieving objectives.[17]

Additionally, the strategic plan document was examined to map enterprise goals, align IT-related objectives, and integrate with COBIT 5 standards, ensuring a cohesive strategy consistent with organizational aspirations and best practices. Leveraging insights from the organizational structure, a Responsible, Accountable, Consulted, and Informed (RACI) chart was developed to clarify roles and responsibilities, enhance collaboration, and ensure accountability throughout the assessment. The RACI chart also helped in determining respondents for this research, which included key personnel such as the library head and IT head.

This assessment was conducted from November 2023 to January 2024, involving document collection, document analysis, observation, and interviews. While the aforementioned documents formed the primary artifacts for this phase, they were complemented by additional materials gathered during the observation and interview stages.

The organizational structure and decision-rights context were used to identify key stakeholders and select respondents most directly involved in DSS01 and DSS05 activities. As shown in Table 1, the head of library IT (HLIT) is primarily responsible (R) for executing operational and security processes, while accountability (A) is assigned to the head of library administration or head of library services (HL) for certain subprocesses. Senior leadership (rector, deputy rector for academic affairs, deans) and other library division heads are generally informed (I) to ensure institutional alignment.

Importantly, this RACI mapping also guided the selection of respondents for the study. Individuals in Responsible or Accountable roles for DSS01 and DSS05 were chosen to provide the most relevant and informed perspectives during interviews and questionnaire responses.

Beyond identifying respondents, Table 1 highlights a governance pattern in which operational and security execution is heavily concentrated in the head of library IT, while formal accountability (A) is not consistently assigned across several DSS01 or DSS05 subprocesses. This concentration increases dependency on a single role and can weaken escalation clarity, prioritization, and cross-unit coordination—especially in a centralized institutional IT environment. To support movement toward capability level 3, the analysis shows that the library should formalize process ownership (Accountable roles) for each DSS01 and DSS05 subprocess (e.g., service continuity ownership for core library systems and clear accountability for security monitoring and incident response) and define structured consultation paths with central IT for shared infrastructure and enterprise security controls.

Table 1. RACI table.

	Roles*								
Domain & Subprocess	**Rec**	**DR-Ac**	**Dean**	**HL**	**HLA**	**HLIT**	**HLS**	**HCD**	**HFB**
DSS01 – Manage Operations									
DSS01.1 Perform IT operational procedures	I	I	I	I	I	R	I	I	I
DSS01.2 Manage outsourced IT services**	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
DSS01.3 Monitor IT infrastructure	I	I	I	A	I	R	I	I	I
DSS01.4 Manage IT environment	I	I	I	I	I	R	I	I	I
DSS01.5 Manage IT facilities	I	I	I	I	I	R	I	I	I
DSS05 – Manage Security Services									
DSS05.1 Protect against malware	I	I	I	I	I	R	I	I	I
DSS05.2 Manage network and connectivity security	I	I	I	I	I	R	I	I	I
DSS05.3 Manage endpoint security	I	I	I	I	I	R	I	I	I
DSS05.4 Manage user identity and logical access	I	I	I	I	I	R	I	I	I
DSS05.5 Manage physical access to IT assets	I	I	I	I	I	R	I	I	I
DSS05.6 Manage sensitive documents and output devices	I	I	I	I	I	R	I	I	I
DSS05.7 Monitor infrastructure for security-related events	I	I	I	A	I	R	I	I	I

*Roles: Rec = Rector, DR-Ac = Deputy Rector for Academic Affairs; Dean = Dean of Faculty; HL = Head of Library; HLA = Head of Library Administration; HLIT = Head of Library IT; HLS = Head of Library Services; HCD = Head of Collection Development; and HFB = Head of Faculty Library Branch.

** DSS01.2 (Manage outsourced IT services) is excluded from assessment because outsourced operational services are not used and are not within the assessment scope at UNRI Library.

RESULTS

Results of DSS01 (Manage Operations) and DSS05 (Manage Security Services) are crucial in assessing the IT governance processes at the UNRI Library. The evaluation is based on two key aspects: base practices and work products.

For DSS01, the base practices ratings were 3.00 (HL) and 2.50 (HLIT), producing an overall mean of 2.75 (Table 2). Using the scoring rules described in the Analysis Processes section, this aggregated score is categorized as partially achieved (P) for base practices. The work products ratings were 3.75 (HL) and 2.75 (HLIT), producing an overall mean of 3.25, categorized as largely achieved (L) (Table 3). Following the COBIT assessment logic that the overall result is constrained by the weaker evidence set, DSS01 is determined by the base practices rating and is therefore reported at capability level 0.

Table 1. The results of the base practices evaluation for DSS01.

Respondent	Base Practices Scale
HL	3.00
HLIT	2.50
Scale Value	2.75
NPLF Scale	**P**

Table 2. The results of the work product evaluation for DSS01.

Respondent	Work Product Scale
HL	3.75
HLIT	2.75
Scale Value	3.25
NPLF Scale	**L**

HL = head of library; HLIT = head of library IT

For DSS05, the base practices ratings were 3.29 (HL) and 3.14 (HLIT), producing an overall mean of 3.21 and categorized as largely achieved (L) (Table 4). The work products ratings were 4.00 (HL) and 2.86 (HLIT), producing an overall mean of 3.43, also categorized as largely achieved (L) (Table 5). Because both evidence sets meet at least the L rating, DSS05 is reported at capability level 1, with the overall result constrained by the smaller of the two aggregated ratings.

Table 4. The results of the base practices evaluation for DSS05.

Respondent	Base Practices Scale
HL	3.29
HLIT	3.14
Scale Value	3.21
NPLF Scale	**L**

Table 5. The results of the work product evaluation for DSS05.

Respondent	Work Product Scale
HL	4.00
HLIT	2.86
Scale Value	3.43
NPLF Scale	**L**

HL = head of library; HLIT = head of library IT

Gap analysis is then conducted to identify the variance between the current capability levels and the desired levels. For this study, the desired capability level for both DSS01 and DSS05 is set at level 3, based on an internal benchmark and agreement with key stakeholders from the institution and library. While this target is not a formally published goal of the institution, it reflects the benchmarked standard that the institution aims to achieve in the medium term. Table 6 presents the gap analysis between the current and target capability levels for DSS01 and DSS05.

Table 6. The gap analysis between current capability level and target capability level.

Domain	COBIT 5 Domain Process Description	Current Capability Level (a)	Target Capability Level (b)	Gap (b–a)
DSS01	Manage Operations	0	3	3
DSS05	Manage Security Services	1	3	2

In conclusion, the capability assessment indicates that DSS01 is at level 0 with a score of 2.75 on the P scale, while DSS05 is at level 1 with a score of 3.21 on the L scale. To bridge the gaps and achieve the desired target levels, recommendations need to be formulated, focusing on advancing through levels 1, 2, and 3 for DSS01 and levels 2 and 3 for DSS05. This underscores the need for strategic improvement efforts in IT governance processes at the UNRI Library.

RECOMMENDATIONS FOR IMPROVEMENTS

In the context of enhancing the IT capabilities at the UNRI Library, a comprehensive analysis has been conducted to identify key process areas and associated practices necessary for operational excellence. This analysis focuses on critical IT management and security processes, ensuring robust operational activities and safeguarding the library's digital infrastructure. The recommendations in Tables 7 and 8 were developed by mapping the gaps identified in the DSS01 and DSS05 assessments to COBIT 5 expected practices and work products, then tailoring the actions to the operational realities of a university library (e.g., integrated library systems, circulation and cataloging workflows, access to e-resources, institutional repositories, and user account provisioning). While the structure of the recommendations aligns with COBIT 5, the implementation examples and prioritization reflect evidence observed during document review and interviews within the library context.

Table 7. Recommendations based on base practices and work product for DSS01 and DSS05.

Process Area	Base Practice	Work Product
DSS01	Ensure IT operations follow established standard operating procedures (SOPs), including scheduled infrastructure maintenance, data backups, and environmental protection procedures, to maintain system reliability and prevent disruptions or data loss.	Work products such as SOPs, monitoring reports, security policies, and asset evaluations support systematic, secure, and efficient IT operations for the library.
DSS05	Implement preventive and security measures to protect IT systems, secure endpoints, and control user access, ensuring the integrity and confidentiality of library data.	Security policies, device evaluations, access reports, and monitoring documents form a robust framework that protects the library's digital assets and user trust.

The UNRI Library enhances its IT capabilities through strong management performance and process standardization. Table 8 outlines key aspects of management performance, output,

process definitions, and applications for critical IT areas, ensuring enforcement, evaluation, and standardization of IT operations and security to maintain efficiency, security, and reliability.

Table 8. Recommendations based on management performance, management output, and process standard definition and application for DSS01 and DSS05.

Process Area	Management Performance	Management Output	Process Standard Definition	Process Standard Application
DSS01	Enforce IT operations, monitoring, environmental protection, and asset management per standard operating procedures (SOPs).	Evaluate IT operations, monitoring, environmental protection, and asset management per SOPs.	Define standards for IT operations, monitoring, environmental protection, and asset management.	Apply standards by implementing planned maintenance for the integrated library system/ online public access catalog and discovery systems based on the academic calendar, running automated daily backups of the library database and institutional repository with off-site copies, monitoring uptime and response times for key public services (catalog search, circulation, and e-resource access) with clear alert thresholds, and maintaining weekly operational checklists with quarterly SOP compliance reviews.
DSS05	Enforce preventive measures, security, endpoint security, access rights, physical security, and IT monitoring per SOPs.	Evaluate preventive measures, security, endpoint security, access rights, physical security, and IT monitoring per SOPs.	Define standards for preventive measures, security, endpoint security, access rights, physical security, and IT monitoring.	Apply standards by setting role-based access for key library functions (circulation, cataloging, acquisitions, and admin), requiring multi-factor authentication for all privileged access (including remote access), regularly reviewing login and proxy logs for unusual activity, keeping a security incident log for library systems with clear response time targets, and securing any server rooms or network closets that support library services.

These recommendations were reviewed and discussed with key stakeholders from the institution, including representatives from the library and IT department. The institution expressed interest in adopting these measures as part of its continuous improvement efforts. In line with the internal benchmark established in this study, the institution aims to operate at capability level 3 for both

DSS01 and DSS05. By progressively implementing these recommendations, the institution can enhance its IT governance framework, improve operational efficiency, mitigate risks, and align IT activities with organizational objectives, ultimately supporting the institution's academic mission and strategic goals.

CONCLUSION

The assessment of IT governance at the UNRI Library provided key insights into the institution's IT processes and capabilities. The analysis highlighted strengths and areas needing improvement, particularly in the DSS01 and DSS05 domains, focusing on operational IT activities, security, infrastructure monitoring, and risk management. The evaluation also examined compliance with the COBIT 5 framework, revealing alignment in some areas but deficiencies in standardized procedures and performance monitoring. Key improvement areas include defining standard processes, ensuring adherence, enhancing security measures, and optimizing resource management to strengthen the overall IT governance framework.

Based on the assessment, recommendations were made to improve process capabilities within the DSS domains, focusing on SOP implementation, procedure standardization, performance management, and output evaluation. The analysis highlights the importance of standardization and compliance with IT governance frameworks like COBIT 5, which ensure consistency, efficiency, accountability, and risk mitigation. Continuous monitoring and evaluation of IT processes are crucial for tracking progress, identifying issues, and adapting to technological changes, enabling timely corrective actions to prevent disruptions or security breaches.

In conclusion, the analysis of IT governance within the UNRI Library offers valuable insights into current processes, compliance status, and areas for improvement. By implementing the recommended enhancements and fostering a culture of continuous improvement, the UNRI Library can bolster its IT governance framework, enhance operational efficiency, and better support its academic mission and institutional objectives.

ENDNOTES

[1] Rodrigo Humberto Del Pozo Durango et al., "Analysis of Information Security Governance for Higher Education Institutions," in *2023 Asia Conference on Cognitive Engineering and Intelligent Interaction (CEII)* (IEEE, 2023), 29–34, https://doi.org/10.1109/CEII60565.2023.00014.

[2] Ita Arfyanti, Nursobah Nursobah, and Rajiansyah Rajiansyah, "IT Governance of Senayan Library Management System (SLiMS) Library and Archives Department of East Kalimantan Province Using COBIT 5.0," *Jurnal Ilmiah MATRIK* 23, no. 2 (2021): 159–67, https://doi.org/10.33557/jurnalmatrik.v23i2.1429.

[3] Kamaludin Kamaludin and Abdurachman Prasetyadi, "Science Mapping of Library and Information Science (LIS) and Library Technology Studies in Indonesia," *Al-Ma'mun Jurnal Kajian Kepustakawanan dan Informasi* 4, no. 1 (2023): 1–15, https://doi.org/10.24090/jkki.v4i1.7145.

[4] Jonhariono Sihotang, Erwin Setiawan Panjaitan, and Roni Yunis, "Evaluation of Information Technology Governance by Using COBIT 5 Framework at Higher Education," *Jurnal Mantik* 4, no. 3 (2020): 2194–203.

[5] Durango et al., "Analysis of Information Security Governance for Higher Education Institutions."

[6] Pierre Bernard, *COBIT® 5-A Management Guide* (Van Haren, 2012).

[7] ISACA, *COBIT 5* (ISA, 2012).

[8] Bernard, *COBIT® 5-A Management Guide*.

[9] Ana Irhandayaningsih, "Performance Measurement of Information Technology Governance in the Library of Diponegoro University Using COBIT Assessment Framework," *E3S Web of Conferences* 202 (2020): 15001, https://doi.org/10.1051/e3sconf/202020215001.

[10] ISACA, *COBIT 5: Process Assessment Model (PAM): Using COBIT 5* (ISACA, 2013).

[11] Huishu Wu and Chuan Zhang, "Reconstructing the Definition of Audit," in *Audit the Audit: Redefining the Concept of Audit in the Context of Personal Data Protection* (Springer, 2025), 107–74.

[12] Arfyanti, Nursobah, and Rajiansyah, "IT Governance of Senayan Library Management System."

[13] Irhandayaningsih, "Performance Measurement of Information Technology Governance."

[14] Godwin Nzeako et al., "Theoretical Insights into IT Governance and Compliance in Banking: Perspectives from African and US Regulatory Environments," *International Journal of Management & Entrepreneurship Research* 6, no. 5 (2024): 1457–66, https://doi.org/10.51594/ijmer.v6i5.1094.

[15] Percy Masibigiri, Alex Dandadzi, and Solly Seeletse, "The Adoption of Information Technology Governance Frameworks by Universities in Gauteng Province, South Africa," *International Journal of Research in Business and Social Science* 13, no. 7 (December 8, 2024): 492–99, https://doi.org/10.20525/ijrbs.v13i7.3643.

[16] Solmaz Derogar Kalkhoran et al., "Providing a Governance Model for Information Technology (COBIT) in the Enterprise Architecture of Iran Public Libraries Foundation," *International Journal of Information Science and Management* 23, no. 3 (February 26, 2025): 1–21, https://doi.org/10.22034/ijism.2025.2048634.1672.

[17] Tim Perpustakaan Uniersitas Riau, "Dokumen Rencana dan Strategis Perpustakaan Universitas Riau Tahun 2023" (December 20, 2023), https://lib.unri.ac.id/wp-content/uploads/2024/11/SK-STRATEGIS-BISNIS.pdf.