

COBIT 2019 DSS BEST PRACTICES FOR SUSTAINABLE POINT-OF-SALE SYSTEMS: A SYSTEMATIC REVIEW

Alfredo Valentino Setiawan¹, Antonius Wahyu Sudrajat^{2*}, Dafid³

^{1,2,3}Master of Information Systems Study Program, Universitas Multi Data Palembang, South Sumatra, Indonesia

Corresponding Author : Wahyu.sudrajat@mdp.ac.id

ABSTRACT

Food and beverage businesses increasingly depend on Point of Sale systems, yet daily Point of Sale operations are frequently conducted without formal information technology governance. This study reviews how the Control Objectives for Information and Related Technologies two thousand nineteen Deliver, Service, and Support domain has been assessed in practice and what it offers for governing Point of Sale operations. Following the Preferred Reporting Items for Systematic Reviews and Meta Analyses two thousand twenty protocol, one hundred eighty six records from Google Scholar published between two thousand twenty one and two thousand twenty six were screened, leading to thirty four peer reviewed studies being synthesized. Reported operational risks were organized using Risk and Control Self Assessment logic, linking each identified risk directly to a specific Deliver, Service, and Support control objective. Most assessed organizations currently operate at capability level one, representing performed status, or level two, representing managed status, which falls one to three levels below their target operational capability, while few studies translate assessment results into practical procedures. Three recurring risk clusters emerged: infrastructure failure, security weaknesses, and software and data integrity problems. From these findings, the study derives a comprehensive five pillar standard operating procedure framework covering domain objectives Deliver, Service, and Support zero one through Deliver, Service, and Support zero six. Because only two included studies explicitly focus on food and beverage settings, the framework should be understood as a transferable starting point requiring pilot testing in food and beverage businesses prior to broader operational deployment.

Keywords: COBIT 2019, Deliver Service and Support, Risk and Control Self-Assessment, Point of Sale, Systematic Literature Review

INTRODUCTION

The rapid growth of information technology (IT) has made information a central business resource, and organizations adopt IT mainly to improve the performance of their business processes (Erlansari et al., 2023). Adoption alone, however, does not guarantee that IT supports business goals. Weak alignment is a common cause of failed digital transformation; about 70% of IT projects are reported to miss their initial targets because of poor coordination and weak governance controls (Archaqie & Pratiwi, 2025). Many organizations still show weaknesses in operational implementation and continuous control (Alfitanaya et al., 2024), which suggests that a governance framework on paper is not enough without routine control of daily operations.

IT has also become part of business strategy, which calls for governance that is structured, focused on risk mitigation and resource efficiency, and aligned with long-term business goals (Putra, 2025). In the food and beverage (FnB) sector, one of the most widely used technologies for daily operations is the *Point of Sale* (POS) system. A POS system is more than a digital cash register; it is the central record of

daily sales, payments, and stock movements. Its reliability depends not only on the software but on a Standard Operating Procedure (SOP), a written guideline that defines how work is carried out so that each step is performed consistently and in line with the organization's quality requirements (Sukanto et al., 2021).

SOPs matter for POS use because they act as instruments of control. Without clear procedures, missing controls open the door to fraud, data manipulation, and slow handling of technical problems (Erlansari et al., 2023; Fawwazdzaky et al., 2025), and the validity of POS transaction data can no longer be assured. COBIT 2019 offers a recognized set of governance and management objectives for such controls, and its Deliver, Service, and Support (DSS) domain addresses exactly the daily operation, incident handling, continuity, security, and business process controls that a POS environment needs. Yet adaptation of COBIT 2019 to micro, small, and medium enterprises (MSMEs) and retail settings is still limited, and many organizations continue to rely on manual procedures and incomplete policy documentation (Arhaqie & Pratiwi, 2025; Putra, 2025). Operational risk management guidance such as *Risk and Control Self-Assessment* (RCSA), which asks process owners to identify their own risks and the controls that address them, is also rarely combined with COBIT assessments, even though early identification of operational risk is known to protect business objectives (Haryanti & Hutomo, 2024).

A previous systematic review of COBIT 2019 summarized implementation challenges and benefits across industry sectors (Antariksa et al., 2025), but it did not focus on the operational DSS domain or translate findings into procedures that small businesses can use. Most individual COBIT 2019 studies also stop at reporting capability levels and gaps without proposing operational procedures (Amrullah et al., 2025). This review addresses that gap with three contributions: it focuses on the DSS domain, it organizes reported risks with RCSA logic, and it converts the evidence into a draft SOP framework for POS operations in FnB businesses. The review is guided by three research questions (RQs). RQ1: What trends in capability levels and governance gaps are reported for the DSS domain in previous studies? RQ2: Which operational risks recur in these studies, and how can they be organized with RCSA logic within COBIT 2019? RQ3: Which DSS best-practice elements can be synthesized into a draft SOP that sustains POS operations?

METHODS

This systematic literature review follows the PRISMA 2020 (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) reporting guideline, which was designed to ensure transparency and completeness in reporting how studies were identified, selected, and synthesized (Page et al., 2021). The flow diagram in Figure 1 reports the number of records identified, screened, assessed for eligibility, and included.

Data Source and Search Strategy

Google Scholar was used as the literature source because it indexes the national Indonesian journals in which most COBIT 2019 case studies are published, and the search was run through *Harzing's Publish or Perish* software. The search string was "COBIT 2019" AND ("Audit" OR "Tata Kelola TI"), where *Tata*

Kelola TI is the Indonesian term for IT governance, so that both English- and Indonesian-language studies were captured. The search was limited to publications from 2021 to 2026 to capture recent practice. The search covered publications available up to January 2026, the publication date of the most recent included study.

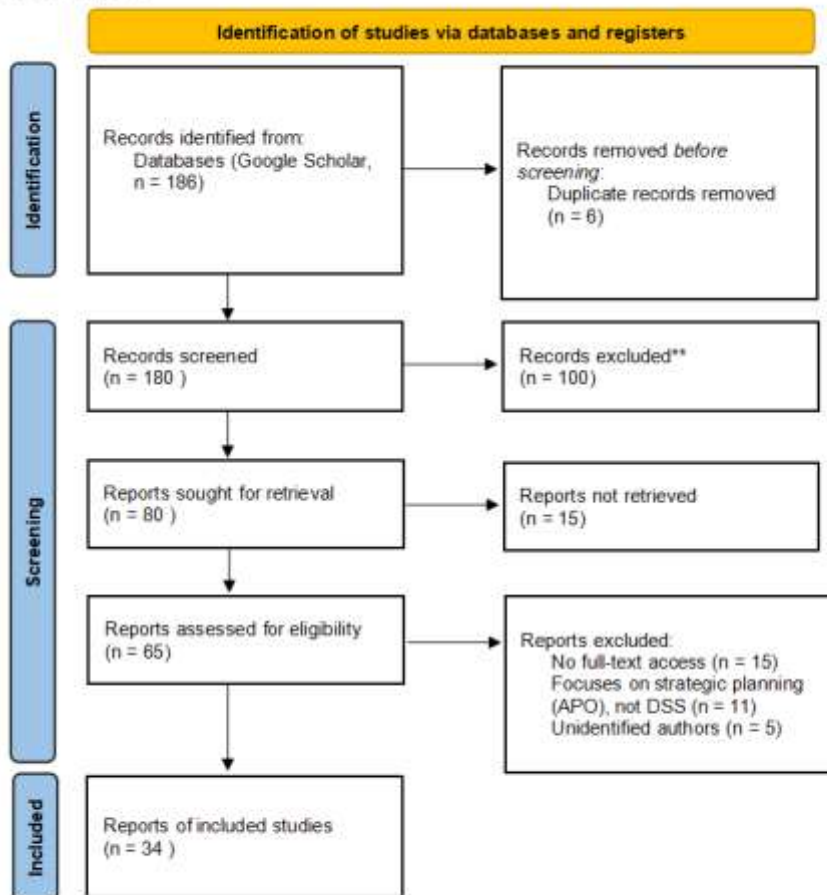
Eligibility Criteria

Studies were included if they were published between 2021 and 2026, applied COBIT 2019 in an organizational assessment or design, were peer-reviewed, and were available in full text. Studies were excluded if they were published before 2021, were weakly related to the topic, were not peer-reviewed, were not available online, or did not address any DSS objective. A small number of additional sources are cited only for background, method, or context (for example, the PRISMA statement, an ISO 31000 risk study, a COBIT 5 security study in an FnB company, and an earlier COBIT 2019 review); these are not counted among the 34 included studies.

Study Selection Process

The search returned 186 records from Google Scholar. After 6 duplicates were removed, 180 records were screened by title and abstract, and 100 unrelated or irrelevant records were excluded. Of the 80 reports sought for retrieval, 15 could not be retrieved. The remaining 65 reports were assessed in full: 15 were excluded because the full text was not accessible, 11 because they did not address the operational DSS domain and focused instead on strategic planning (APO) or high-level governance (EDM), and 5 because the author or publisher identity was unclear. This process yielded 34 studies that met all criteria (Figure 1). Screening and eligibility assessment were performed by the authors against the predefined criteria.

PRISMA Report



Source: Page MJ, et al. BMJ 2021;372:n71. doi: 10.1136/bmj.n71.

This work is licensed under CC BY 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>

Figure 1. PRISMA 2020 Flow Diagram of the Study Selection Process

Source: Adapted from Page et al. (2021)

Data Extraction and Synthesis

For each study, the following data were extracted: (1) authors and year, (2) organization and sector, (3) COBIT objectives assessed, (4) method, (5) reported capability or maturity levels and target levels, and (6) reported risks and recommendations. The synthesis followed three steps that match the research questions. First, reported as-is and to-be levels were compared across studies to describe capability trends and gaps (RQ1). Second, every risk statement reported in the studies was coded, grouped into risk clusters, and paired with the DSS objective whose controls address it. This pairing follows RCSA logic, in which each identified risk is linked to an owner-level control that can be self-assessed (RQ2). Third, the recommended practices attached to each DSS objective were consolidated into SOP elements (RQ3). No formal risk-of-bias tool was applied because the included studies are descriptive case assessments; instead, peer-review status and publisher identity were used as minimum quality criteria.

RESULT AND DISCUSSION

Characteristics of the Included Studies

The 34 included studies were published between 2021 and 2026 and cover the public sector, higher education, health care, logistics and distribution, transport, and MSMEs. Most are single-organization case studies that use the COBIT 2019 capability assessment, and almost all were published in Indonesian national journals. Only two studies concern FnB businesses directly: an audit of the POS system at Kafe Batas (Gunawan et al., 2025) and a security governance evaluation at PT Tsabita Cake (Habiba et al., 2021), the latter based on COBIT 5. The evidence used for the POS-oriented synthesis is therefore largely drawn from other sectors whose DSS processes, such as service operations, incident handling, and transaction control, are comparable to those of a POS environment.

Trends in IT Governance Capability Levels and Gaps (RQ1)

Capability targets in the reviewed studies were set to keep technology management aligned with organizational strategy, above all to keep services stable and reliable for users (Purnama & Akbar, 2025). Table 1 summarizes the levels reported for operational governance. The comparison of as-is and to-be levels shows a consistent pattern across sectors (Erlansari et al., 2023; Ulfadinata & Panjaitan, 2024).

Table 1. Capability Levels Reported for Operational Governance in the Reviewed Studies

Organization (sector)	Process focus	Reported level	Source
Regency communication and informatics office (public sector)	COBIT 2019 audit incl. DSS	1 (Performed)	Afifah et al. (2025)
Data and information center of a ministry (public sector)	Governance design incl. DSS	1 (Performed)	Afdhani & Soewito (2024)
Universities and higher-education units (education)	MEA and DSS	1 (Performed)	Windasari et al. (2022); Priyatna & Sanwani (2024)
CV Bangun Techno (IT equipment distributor)	Selected COBIT 2019 objectives	2 (Managed)	Putra (2025)
PT XYZ (operational information system)	Operational audit	2 (Managed)	Herawati et al. (2026)
Kafe Batas (FnB, POS system)	POS audit incl. APO12, DSS01	2–5 across processes	Gunawan et al. (2025)
PT XYZ (web-based products)	DSS domain	2–4 (maturity)	Noor et al. (2022)
Universitas Sriwijaya Library (education)	IT service maturity	3 (Established)	Aleksi & Afrina (2023)
STMIK Lombok (education)	Academic data governance	3 (Established)	Amrullah et al. (2025)
PT Angkasa Pura Indonesia (airport operator)	DSS02	4 (Predictable)	Hidayah, Amany, & Adila (2025)

Dominance of Low Capability Levels (Levels 1 and 2)

Most studies report that IT governance in the public sector, education institutions, and MSMEs remains at a basic level (Afifah et al., 2025), and weak implementation was also found in universities (Wijaya et al., 2023; Edi et al., 2025). Organizations such as a regency communication and informatics office, a

ministry data and information center, and several universities were assessed at Level 1 (Performed) (Erlansari et al., 2023; Windasari et al., 2022; Priyatna & Sanwani, 2024; Afdhani & Soewito, 2024). At this level, processes achieve their purpose through activities that are not formally organized and are largely reactive. Entities such as CV Bangun Techno and PT XYZ had reached Level 2 (Managed), where procedures are documented but not yet standardized across units (Putra, 2025; Herawati et al., 2026). The audit of the Kafe Batas POS system reported levels from 2 to 5 across processes, with the largest gaps in risk management (APO12) and service operations (DSS01) (Gunawan et al., 2025). An evaluation of web-based products at another company likewise reported maturity values between 2 and 4 in the DSS domain (Noor et al., 2022).

Medium-to-High Capability Levels (Levels 3 and 4)

Only a few studies report more mature levels. Level 3 (Established) was found in organizations with well-defined SOPs, such as the Universitas Sriwijaya Library and STMIK Lombok (Aleksi & Afrina, 2023; Amrullah et al., 2025). The highest level was reported for PT Angkasa Pura Indonesia, an operator of critical infrastructure, which reached Level 4 (Predictable) in DSS02 through data-driven management and quantitative performance measurement (Hidayah, Amany, & Adila, 2025). The common factor in these cases is the presence of documented and enforced procedures, which supports the view that SOPs are the practical step between Level 2 and Level 3.

Gap Analysis

The synthesis reveals an empirical gap: most organizations operate at capability level 1 or 2, while their targets are usually level 3 or 4, a difference of one to three levels (Erlansari et al., 2023; Aleksi & Afrina, 2023). Although IT has been implemented, daily operations remain reactive and lack formal documentation (Windasari et al., 2022; Afdhani & Soewito, 2024; Herawati et al., 2026). The review also reveals a research gap. Current studies concentrate on public-sector and institutional audits and give little attention to digital MSMEs and the FnB sector (Putra, 2025; Archaqie & Pratiwi, 2025), and most stop at assessment results without proposing procedural solutions (Amrullah et al., 2025). These two gaps motivate the SOP synthesis in RQ3.

RCSA-Based Operational Risk Profile within COBIT 2019 (RQ2)

Low capability in the DSS domain goes hand in hand with frequent IT service disruptions (Alfitanaya et al., 2024; Rahadiani et al., 2025). Coding the risk statements reported in the studies produced three recurring clusters. For each cluster, the RCSA view asks which control should exist at the process-owner level and which DSS objective provides it; the resulting pairs are summarized in Table 2.

Infrastructure Failure and Hardware Damage

Hardware incidents and network disruptions were rated as "very high" risks in several organizations (Sahara et al., 2025; Harjo et al., 2023). The absence of automatic failover and weak backup arrangements were the main reasons services did not recover quickly after disruptions to servers or network devices (Alfitanaya et al., 2024; Afdhani & Soewito, 2024).

Downtime impact. PT Angkasa Pura Indonesia reported system downtime averaging 4.3 hours per month, above its operational tolerance (Hidayah, Amany, & Adila, 2025). In a library system, the lack of dedicated maintenance staff made disruption handling unsustainable (Aleksi & Afrina, 2023).

Capacity risk. In a national tax system, weak infrastructure management left the system unable to handle peak loads because of limited active backup (Alfitanaya et al., 2024), and a ministry data center reported frequent network device failures that disrupted user access (Afdhani & Soewito, 2024). For a POS environment, the equivalent risks are terminal or network failure during peak hours, which stop sales directly.

Cyberattacks and Security Vulnerabilities

Weak security service controls (DSS05) expose organizations to logical attacks (Fawwazdzaky et al., 2025). Universitas Nurdin Hamzah experienced a system breach in mid-2024 that disrupted services and redirected users to unauthorized sites (Sahara et al., 2025). Data leakage becomes more likely when security policies are not formally documented and incidents are handled only after they occur (Andriana et al., 2025).

Malware and ransomware. An organization in the air transport sector was paralyzed for 8 hours by a ransomware attack (Hidayah, Amany, & Adila, 2025). In a maintenance, repair, and overhaul (MRO) company, malware and industrial espionage were rated as medium-to-high risks that required a strict internet-use procedure (Fawwazdzaky et al., 2025).

Access and vendor vulnerabilities. At PT Tsabita Cake, an FnB company, vulnerabilities stemmed from unstable network connectivity and the absence of a requirement for antivirus software on user devices (Habiba et al., 2021). These risks are worsened by low staff awareness of security protocols and the lack of regular penetration testing (Habiba et al., 2021; Priyatna & Sanwani, 2024). Unsupervised dependence on external vendors adds a further risk when providers cannot guarantee data confidentiality or continuity during disruptions on their side (Hidayah, Firdia, et al., 2025), a situation common among FnB businesses that use cloud-based POS services.

Software Malfunction and Data Integrity

Application instability and disorganized data management threaten the accuracy of business information (Afdhani & Soewito, 2024; Rahadiani et al., 2025). System bugs and access overloads can make systems completely inaccessible (Afdhani & Soewito, 2024).

Dependence on manual procedures. At STMIK Lombok, manual and non-integrated data management slowed access to information and increased the risk of losing primary data (Amrullah et al., 2025). At PT XYZ, operations that depend on manual procedures were found likely to cause transaction recording errors (Herawati et al., 2026).

Data integrity and manipulation. Weak user access controls allow both accidental software changes and deliberate data manipulation leading to fraud (Fawwazdzaky et al., 2025). Without complete audit logs, organizations struggle to investigate data security incidents (Alfitanaya et al., 2024). In POS

operations, this cluster corresponds to unauthorized voids, discounts, and price changes, which are typical channels of cashier fraud.

Synthesis of DSS Best Practices for POS System SOPs (RQ3)

The recommendations attached to each DSS objective in the reviewed studies were consolidated into five SOP pillars (Table 2). Each pillar answers one or more of the risk clusters identified in RQ2.

Table 2. RCSA-Based Mapping of Recurring Risks to DSS Practices and Proposed SOP Elements

Risk cluster (RQ2)	DSS objective	Proposed SOP element (RQ3)	Main sources
Unmonitored daily operations; inconsistent workflows	DSS01	Opening and closing checklist for POS terminals; daily infrastructure monitoring; periodic workflow review	Thenu & Rudianto (2024); Mariatama et al. (2022)
Slow handling of terminal and network failures	DSS02	Ticket logging with SLA targets; first-level and escalation paths	Ulfadinata & Panjaitan (2024); Wahyudi & Sutedi (2025)
Recurring disruptions; long downtime; no failover	DSS03, DSS04	Root cause analysis for repeated incidents; scheduled transaction backup; tested recovery plan	Hidayah, Amany, & Adila (2025); Alfitanaya et al. (2024)
Malware, ransomware, weak access control, vendor dependence	DSS05	Role-based (least-privilege) user accounts; antivirus and patch routine; vendor access supervision	Habiba et al. (2021); Fawwazdzaky et al. (2025); Sahara et al. (2025)
Manual recording, input errors, data manipulation and fraud	DSS06	Automated transaction validation; audit logs; void and discount authorization; staff procedure training	Radja et al. (2025); Beato & Fianty (2024); Herawati et al. (2026)

Pillar 1: Operations Stability and Daily Monitoring (DSS01)

Studies in the logistics sector show that standard operating procedures in DSS01 keep workflows efficient and ensure that every transaction is recorded systematically (Thenu & Rudianto, 2024; Mariatama et al., 2022). Daily monitoring of infrastructure performance reduces system errors and keeps services reliable (Ulfadinata & Panjaitan, 2024; Wahyudi & Sutedi, 2025), and periodic workflow review improves overall operational efficiency (Alfitanaya et al., 2024; Thenu & Rudianto, 2024). For a POS environment, this translates into opening and closing checklists for terminals, printers, and network devices.

Pillar 2: Incident and Service Request Handling (DSS02)

Documented incident handling procedures are needed so that every disruption to the transaction system is resolved within a time frame defined in a service level agreement (SLA), supported by a clear escalation path from first-level staff to the relevant technical unit or vendor (Ulfadinata & Panjaitan, 2024; Wahyudi & Sutedi, 2025). The Level 4 result reported for DSS02 at PT Angkasa Pura Indonesia shows the value of measuring incident handling quantitatively (Hidayah, Amany, & Adila, 2025).

Pillar 3: Problem Investigation and Service Continuity (DSS03 and DSS04)

Best practice in DSS03 requires identifying the root causes of repeated disruptions so that they do not recur, while DSS04 keeps the system available through routine backup of transaction data and a tested recovery plan (Ulfadinata & Panjaitan, 2024; Wahyudi & Sutedi, 2025). For POS operations, the continuity

plan should include an offline sales procedure that allows transactions to be recorded and synchronized once the system is restored.

Pillar 4: Security Operations and Access Rights Management (DSS05)

The SOP should govern user identities and access rights according to each person's responsibilities, following the least-privilege principle, and should require routine prevention, detection, and correction measures against malicious software (Ulfadinata & Panjaitan, 2024; Wahyudi & Sutedi, 2025). Vendor access to POS systems should be supervised and logged (Hidayah, Firdia, et al., 2025).

Pillar 5: Business Process Controls and Data Validation (DSS06)

A study at a regional hospital recommends automated controls on transaction processes to maintain data accuracy and reduce operational bottlenecks (Radja et al., 2025), and research in the distribution sector shows that operational knowledge management helps reduce input errors by front-line staff (Beato & Fianty, 2024). Better information system performance also depends on staff compliance with established procedures (Thenu & Rudianto, 2024). For POS operations, this pillar covers automated validation of transactions, authorization rules for voids and discounts, daily reconciliation of sales and payments, and complete audit logs.

Implications and Limitations

Theoretically, this review links two streams that are usually reported separately: COBIT 2019 capability assessment and RCSA-style operational risk control. Practically, the five pillars give FnB owners and managers a checklist that can be adopted step by step, starting with the controls that address their most frequent incidents. Several limitations should be noted. The search used a single database, Google Scholar, so relevant studies indexed only in Scopus, IEEE Xplore, or other databases may have been missed. Nearly all included studies are Indonesian case studies with self-reported assessments, and no formal risk-of-bias tool was applied, which limits generalization. Finally, only two included studies come from FnB settings, so the proposed SOP framework is a transfer of cross-sector evidence and has not yet been validated in FnB businesses.

CONCLUSION

This review of 34 studies shows that operational IT governance assessed with COBIT 2019 is dominated by capability levels 1 and 2, one to three levels below the targets organizations set for themselves, and that the gap is closely related to the absence of documented and enforced procedures. Three risk clusters recur across sectors: infrastructure failure, security weaknesses, and software and data integrity problems. Organizing these risks with RCSA logic links each of them to a DSS control objective, and the resulting five-pillar SOP framework (DSS01 to DSS06) offers FnB businesses a concrete route from reactive to structured POS operations. Future research should pilot the SOP in FnB businesses and measure its effect on incident frequency and transaction errors, extend the search to additional databases, and develop a lightweight, modular COBIT-based assessment for MSMEs that can be combined with automated RCSA data collection.

Acknowledgments

The authors thank the Master of Information Systems Study Program, Universitas Multi Data Palembang, for its academic support during this research.

REFERENCES

- Afdhani, R., & Soewito, B. (2024). Perancangan tata kelola TI menggunakan framework COBIT 2019 pada pusat data dan informasi kementerian [Designing IT governance using the COBIT 2019 framework at a ministry data and information center]. *Jurnal Tata Kelola dan Kerangka Kerja TI*, 10(1), 22–33. <https://ojs.unikom.ac.id/index.php/jtk3ti/article/view/12365>
- Affah, A., Nama, G. F., & Pradipta, R. A. (2025). Implementasi framework COBIT 2019 dalam audit tata kelola teknologi informasi (Studi kasus: Diskominfo Kab. Rejang Lebong) [Implementing the COBIT 2019 framework in an IT governance audit: A case study of the Rejang Lebong Regency Communication and Informatics Office]. *Jurnal Informatika dan Teknik Elektro Terapan*, 13(3S1), 1350–1362. <https://doi.org/10.23960/jitet.v13i3S1.7550>
- Aleksi, & Afrina, M. (2023). Pengukuran tingkat kematangan layanan TI pada UPT Perpustakaan Universitas Sriwijaya menggunakan framework COBIT 2019 [Measuring IT service maturity at the Universitas Sriwijaya Library using the COBIT 2019 framework]. *Jurnal Sistem dan Teknologi Informasi (JustIN)*, 11(3), 389–398. <https://doi.org/10.26418/justin.v11i3.58520>
- Alfitanaya, Fhonna, R. P., & Hasibuan, A. (2024). Implementasi COBIT 2019 dalam meningkatkan tata kelola TI pada website pengelolaan pajak Coretax [Implementing COBIT 2019 to improve IT governance of the Coretax tax management website]. *PRINSIP: Portal Riset & Inovasi Sistem Perangkat Lunak*, 2(2), 110–118. <https://doi.org/10.59696/prinsip.v2i2.146>
- Amrullah, Hendi, M. A., & Nasiri, A. (2025). Perancangan tata kelola data menggunakan COBIT 2019 untuk ketersediaan dan keandalan data akademik [Designing data governance using COBIT 2019 for the availability and reliability of academic data]. *Jurnal Manajemen Informatika & Sistem Informasi (MISI)*, 8(1), 142–153. <https://doi.org/10.36595/misi.v8i1.1407>
- Andriana, D., Firmansyah, G., Tjahjono, B., Widodo, A. M., & Akbar, H. (2025). Audit tata kelola teknologi informasi menggunakan framework COBIT 2019 pada Rumah Sakit Medika Dramaga [IT governance audit using the COBIT 2019 framework at Medika Dramaga Hospital]. *Jurnal Locus: Penelitian & Pengabdian*, 4(8), 8303–8318. <https://locus.rivierapublishing.id/index.php/jl/article/view/4176>
- Antariksa, M. D. S., Angin, M. P., & Widodo, A. P. (2025). COBIT 2019 framework in IT governance: A systematic literature review of implementation challenges and benefits across various industry sectors. *Journal of Renewable Energy, Electrical, and Computer Engineering*, 5(1), 99–105. <https://doi.org/10.29103/jreece.v5i1.19501>

- Archaqie, H. N. R., & Pratiwi, P. (2025). Assessing IT governance in digital UMKM application projects: A comparative study using the COBIT 2019 framework. *Jurnal Ilmiah Sistem Informasi (JUISI)*, 4(2), 232–241. <https://ejurnal.provisi.ac.id/index.php/JUISI/article/view/1036>
- Beato, J., & Fianty, M. I. (2024). COBIT 2019 framework: Evaluating knowledge and quality management capabilities in a printing machine distributor. *Journal of Information Systems and Informatics*, 6(1), 1–12. <https://doi.org/10.51519/journalisi.v6i1.638>
- Edi, N. S. F., Widagdo, A. S., & Putri, N. A. R. (2025). Evaluasi tata kelola teknologi informasi menggunakan COBIT [Evaluating IT governance using COBIT]. *Jatilima: Jurnal Multimedia dan Teknologi Informasi*, 7(4), 913–922. <https://journal.cattleyadf.org/index.php/jatilima/article/view/1793>
- Erlansari, A., Amal, I., & Wijanarko, A. (2023). Efektifitas pengukuran capability level tata kelola teknologi informasi menggunakan kerangka kerja COBIT 2019 [Effectiveness of measuring IT governance capability levels using the COBIT 2019 framework]. *Journal Scientific and Applied Informatics (JSAl)*, 6(2), 297–303. <https://jurnal.umb.ac.id/index.php/JSAl/article/download/5236/3313>
- Fawwazdzaky, R., Nurtrisha, W. A., & Praditya, D. (2025). Analisis IT risk management dengan menggunakan framework COBIT 2019 pada risk profile logical attacks, program and projects lifecycle management, software adoption/usage problems, dan unauthorized actions (Studi kasus: PT XYZ) [IT risk management analysis using COBIT 2019 for selected risk profiles: A case study of PT XYZ]. *Jurnal Ilmiah Penelitian dan Pembelajaran Informatika*, 10(3), 2448–2458. <https://jurnal.stkipgritlungagung.ac.id/index.php/jipi/article/view/6485>
- Gunawan, N. A. F., Zulkarnain, Sangka, Y., & Indaryani, L. (2025). Audit sistem POS Kafe Batas menggunakan framework COBIT 2019 [Auditing the POS system of Kafe Batas using the COBIT 2019 framework]. *Transparansi: Jurnal Ilmiah Ilmu Administrasi*, 8(2), 283–290. <https://doi.org/10.31334/transparansi.v8i2.5375>
- Habiba, A., Saputra, Y. A., & Widodo, A. P. (2021). Evaluasi tata kelola keamanan sistem informasi menggunakan framework COBIT 5 pada PT. Tsabita Cake [Evaluating information system security governance using the COBIT 5 framework at PT Tsabita Cake]. *Jurnal Teknik Informatika dan Sistem Informasi*, 8(2), 908–919.
- Harjo, R. S. D., Kusriani, & Nasiri, A. (2023). Penentuan domain tata kelola IT pada instansi kepegawaian XYZ menggunakan kerangka kerja COBIT 2019 [Determining IT governance domains at civil service agency XYZ using the COBIT 2019 framework]. *Jurnal Teknik Industri*, 9(1), 31–43. <https://doi.org/10.24014/jti.v9i1.21797>
- Haryanti, R. D., & Hutomo, M. (2024). Analisis manajemen risiko operasional berbasis ISO 31000:2018 terhadap perusahaan logistik (Studi kasus JNE Station Center Gedebage Kota Bandung) [ISO 31000:2018-based operational risk management analysis of a logistics company: A case study

- of JNE Station Center Gedebage, Bandung]. *Jurnal Simki Economic*, 7(2), 631–642. <https://doi.org/10.29407/jse.v7i2.709>
- Herawati, T. C., Khaerani, S., Fatihah W, S. S. M., Pradina, M. A., & Pratama, D. (2026). Audit sistem informasi operasional menggunakan framework COBIT 2019 (Studi kasus: PT XYZ) [Operational information system audit using the COBIT 2019 framework: A case study of PT XYZ]. *Saturnus: Jurnal Teknologi dan Sistem Informasi*, 4(1), 30–36. <https://journal.artei.or.id/index.php/Saturnus/article/view/1364>
- Hidayah, N. A., Amany, A. K. D., & Adila, F. (2025). Penilaian tata kelola IT pada PT Angkasa Pura Indonesia berbasis COBIT 2019 dengan domain DSS02 [Assessing IT governance at PT Angkasa Pura Indonesia based on COBIT 2019 domain DSS02]. *Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi*, 11(2), 100–105. <https://doi.org/10.34010/jtk3ti.v11i2.17127>
- Hidayah, N. A., Firdia, N., Rahma, B. A., Azizah, H., & Amanda, D. (2025). Penilaian capability level dan maturity level tata kelola TI pada PT. ABC dengan menggunakan kerangka kerja COBIT 2019 [Assessing IT governance capability and maturity levels at PT ABC using the COBIT 2019 framework]. *Positif: Jurnal Sistem dan Teknologi Informasi*, 11(2). <https://doi.org/10.31961/positif.v11i2.14708>
- Mariatama, A. A., Atrinawati, L. H., & Putra, M. G. L. (2022). Perancangan tata kelola teknologi informasi dengan menggunakan framework COBIT 2019 pada PT JWT Global Logistics Indonesia [Designing IT governance using the COBIT 2019 framework at PT JWT Global Logistics Indonesia]. *Jurnal Sistem Informasi dan Informatika (SIMIKA)*, 5(1), 19–29. <https://ejournal.lppm-unbaja.ac.id/index.php/jsii/article/view/1423>
- Noor, A. Z. M., Widodo, A. P., & Adi, K. (2022). Evaluation of information technology governance using COBIT 2019 on domain DSS (deliver, service, support) at PT XYZ. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, 5(2), 15611–15618. <https://www.bircu-journal.com/index.php/birci/article/view/5465>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., . . . Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, Article n71. <https://doi.org/10.1136/bmj.n71>
- Priyatna, A., & Sanwani. (2024). Penilaian tingkat kapabilitas tata kelola teknologi informasi menggunakan kerangka COBIT [Assessing IT governance capability levels using the COBIT framework]. *Journal Global Technology Computer*, 4(1), 11–20. <https://ejurnal.seminar-id.com/index.php/jogtc/article/view/6321>
- Purnama, D. G., & Akbar, R. I. (2025). Analisis penerapan tata kelola TI menggunakan COBIT 5.0 dan COBIT 2019 [Analysis of IT governance implementation using COBIT 5.0 and COBIT 2019].



JSAl: Journal Scientific and Applied Informatics, 8(2), 372–378.

<https://doi.org/10.36085/jsai.v8i2.8417>

Putra, J. (2025). Analisis dan tata kelola teknologi informasi pada perusahaan distributor peralatan komputer dan jaringan CV Bangun Techno menggunakan framework COBIT 2019 [IT analysis and governance at CV Bangun Techno, a computer and network equipment distributor, using the COBIT 2019 framework]. *Jurnal Ilmiah Sains dan Teknologi*, 2(2), 63–68.
<https://ejournal.ibbi.ac.id/index.php/ST/index>

Radja, C. A. P., Budiraharjo, R., & Chazar, C. (2025). Penerapan COBIT 2019 dalam merancang rekomendasi perbaikan kinerja rumah sakit [Applying COBIT 2019 to design hospital performance improvement recommendations]. *Sistemasi: Jurnal Sistem Informasi*, 14(3), 1176–1185. <https://sistemasi.org/index.php/stmsi/article/view/5076>

Rahadiani, N. A., Nurtrisha, W. A., & Praditya, D. (2025). Analisis perancangan tata kelola teknologi informasi menggunakan kerangka kerja COBIT 2019 pada PT XYZ: Domain BAI06 dan BAI07 [IT governance design analysis using COBIT 2019 at PT XYZ: Domains BAI06 and BAI07]. *Journal of Production, Enterprise, and Industrial Applications*, 3(1), 67–71.
<https://doi.org/10.25124/jpeia.v3i1.9239>

Sahara, E., Fachruddin, & Devitra, J. (2025). Audit tata kelola teknologi informasi Universitas Nurdin Hamzah menggunakan framework COBIT 2019 [IT governance audit of Universitas Nurdin Hamzah using the COBIT 2019 framework]. *Jurnal Ilmiah Media Sisfo*, 19(2), 279–290.
<https://doi.org/10.33998/mediasisfo.2025.19.2.2489>

Sukanto, A. S., Novriando, H., & Reynaldi, A. (2021). Tata kelola teknologi informasi menggunakan framework COBIT 2019 (Studi kasus: UPT TIK Universitas Tanjungpura Pontianak) [IT governance using the COBIT 2019 framework: A case study of the ICT Unit of Universitas Tanjungpura]. *Jurnal Edukasi dan Penelitian Informatika*, 7(2), 210–218.
<https://jurnal.untan.ac.id/index.php/jepin/article/download/47859/75676590292>

Thenu, G. B., & Rudianto, C. (2024). Audit sistem informasi menggunakan framework COBIT 2019 (Studi kasus: PT X) [Information system audit using the COBIT 2019 framework: A case study of PT X]. *Jurnal Teknologi dan Sistem Informasi Bisnis*, 6(4), 762–767.
<https://doi.org/10.47233/jteksis.v6i4.1601>

Ulfadinata, E., & Panjaitan, E. S. (2024). Evaluasi tata kelola TI menggunakan framework COBIT 2019 pada PT. Pundi Mas Berjaya (Jova Software) Medan [Evaluating IT governance using the COBIT 2019 framework at PT Pundi Mas Berjaya (Jova Software), Medan]. *Techno.COM*, 23(3), 502–511. <https://www.researchgate.net/publication/383619151>

Wahyudi, & Sutedi. (2025). Analisis dan pengembangan tata kelola teknologi informasi pada Kantor POS Kotabumi menggunakan COBIT 2019 [Analysis and development of IT governance at the Kotabumi Post Office using COBIT 2019]. *Jurnal Sistem Informasi (JSii)*, 12(1), 10–16.
<https://e-jurnal.lppmunsera.org/index.php/jsii/article/view/9771>





- Wijaya, C., Sukanto, M., Yunis, R., & Megawati. (2023). Audit tata kelola TI menggunakan COBIT 2019 domain APO12 pada Universitas Mikroskil [IT governance audit using COBIT 2019 domain APO12 at Universitas Mikroskil]. *Jurnal SIFO Mikroskil*, 24(2), 197–210.
<https://doi.org/10.55601/jsm.v24i2.1025>
- Windasari, I. P., Rochim, A. F., Alfiani, S. N., & Kamalia, A. (2022). Audit tata kelola teknologi informasi domain monitor, evaluate, and asses dan deliver, service, support berdasarkan framework COBIT 2019 [IT governance audit of the MEA and DSS domains based on the COBIT 2019 framework]. *Jurnal Sistem Informasi Bisnis*, 11(2), 131–138.
<https://doi.org/10.21456/vol11iss2pp131-138>

