International Journal of Contemporary Computer Research (IJCCR), Vol.1, Issue.2 (January, 2025)
ISSN: 2600-9048

Evaluating COBIT 2019-Based IT Governance and Risk Management in a University Environment

Fuad Yehyia Shatat[1], Yazeed Al Moaiad[2]

Faculty of Computer & Information Technology,[1,2]
Al-Madinah International University,
Kuala Lumpur, Malaysia
[1]CC059@lms.mediu.edu.my
[2]yazeed.alsayed@mediu.edu.my

***Abstract*—This study examines how the implementation of COBIT 2019 can enhance information governance, risk management, and technological performance in higher education institutions. Focusing on a medium-sized private higher education institution in Saudi Arabia, the research adopts a mixed-methods design that integrates quantitative survey data from IT personnel, administrators, faculty members, and decision-makers with qualitative insights from structured interviews and document analysis. Governance and management objectives were prioritized using the COBIT 2019 Governance System Design Toolkit, with particular attention to domains related to risk optimization, service continuity, security, and data governance.**

The results show that Managed Risk achieved the highest capability and effectiveness (target level fully achieved), followed by Managed Service Requests and Incidents, and Managed Problems. By contrast, Managed Security Services, Managed Data, and Managed Operations remain relatively weak and exhibit misalignment between desired and actual capability levels. Operational KPIs such as downtime minutes, mean time to repair (MTTR), SLA attainment, and data-loss frequency confirm an asymmetric pattern: risk-related processes are comparatively mature, while data governance and day-to-day operations lag behind.

The study concludes that COBIT 2019 provides a robust reference model for designing and assessing IT governance in universities, but also highlights that achieving higher capability scores in selected domains is not sufficient on its own. Sustainable improvement requires integrated investment in continuity planning, data stewardship, and service management, together with stronger stakeholder engagement and systematic monitoring. The paper contributes empirical evidence from the higher education sector and offers practical recommendations for institutions seeking to leverage COBIT 2019 to support digital transformation, cybersecurity resilience, and institutional performance.

***Keywords*— COBIT 2019, IT governance, information governance, higher education, risk management, service continuity, data governance, Saudi Arabia**

I. INTRODUCTION

Universities increasingly depend on complex information technology (IT) infrastructures to support teaching, learning, research, and administration. Student information systems, learning management systems, research repositories, financial applications, and communication platforms have become mission-critical services. As a result, information governance and IT governance are now central to institutional performance, reputation, and resilience.

However, many higher education institutions struggle to manage IT in a systematic and proactive way. Common challenges include fragmented decision-making, inconsistent risk management, limited visibility into service performance, and weak alignment between IT investments and institutional goals. In this context, structured governance frameworks such as COBIT 2019 offer a promising approach to organizing IT processes, clarifying roles and responsibilities, and defining measurable objectives for control and performance. COBIT 2019, developed by ISACA, provides a comprehensive model for governing and managing enterprise information and technology. It introduces a set of governance and management objectives, design factors, and performance metrics that can be tailored to the specific context of an organization, including universities. For higher education, COBIT 2019 is particularly relevant for managing cybersecurity risks, ensuring continuity and availability of critical services, aligning IT investments with institutional strategies, and monitoring the performance of IT operations.

In the context of digital transformation and national visions that emphasize innovation, quality, and efficiency, universities in Saudi Arabia face pressure to modernize their IT environments while demonstrating strong control over risks. This makes COBIT 2019 not only a theoretical interest but also a practical necessity for institutions that aim to meet accreditation, security, and performance requirements.

A. Problem Statement

In the digital era, universities treat IT as a strategic asset, but often lack mature governance structures to manage associated risks and fully realize the benefits of digital transformation. Without a structured governance framework, institutions may face inefficient use of IT resources, operational disruptions and extended service downtime, cybersecurity vulnerabilities and data-loss incidents, and weak alignment between IT initiatives and strategic goals. The case institution faces precisely these challenges despite significant investments in infrastructure and systems. This raises a core problem: How can COBIT 2019 be used to design, implement, and evaluate an information governance system that improves risk management and technological performance in a university context?

B. Research Questions

The study is guided by the following research questions:

1. How do COBIT 2019 governance and management objectives address cybersecurity risks in university environments?
2. What is the impact of adopting COBIT 2019 on IT risk management practices in universities?
3. How can COBIT 2019 design factors be used to prioritize governance and management objectives in universities?
4. What practical governance and management improvements can be recommended to enhance information governance and digital resilience in universities?

C. Research Objectives

The main objectives of the research are:

1. To analyze how COBIT 2019 governance and management objectives address and mitigate cybersecurity risks in universities, with emphasis on academic systems such as student information systems, research repositories, and administrative applications.
2. To evaluate the impact of adopting COBIT 2019 on risk management practices in IT

processes, especially incident management, service continuity, and data protection.

3. To prioritize governance and management objectives using COBIT 2019 design factors and to identify areas where current capability levels lag behind institutional priorities.
4. To provide practical recommendations for enhancing information governance and digital resilience in higher education institutions.

D. Significance of the Study

The study contributes to both theory and practice. At the theoretical level, it enriches the limited empirical literature on COBIT 2019 in higher education, especially in the context of emerging economies. At the practical level, it offers a structured diagnostic of IT governance performance using COBIT 2019, introduces key performance indicators such as downtime minutes, MTTR, SLA attainment, and data-loss frequency, and provides prioritized recommendations that can guide university leaders, CIOs, and IT managers in strengthening governance, risk management, and digital transformation initiatives.

In addition, the study provides a concrete example of how a university can translate abstract governance principles into measurable actions and improvements, offering a roadmap that other institutions can adapt and refine according to their own context.

E. Hypotheses

Two hypotheses were formulated: H1: The efficiency of technical structures at universities has a significant positive effect on the implementation of IT management and governance procedures, as defined by COBIT 2019. H2: The implementation of the COBIT 2019 framework significantly improves institutional performance by reinforcing control over information technology and mitigating associated risks.

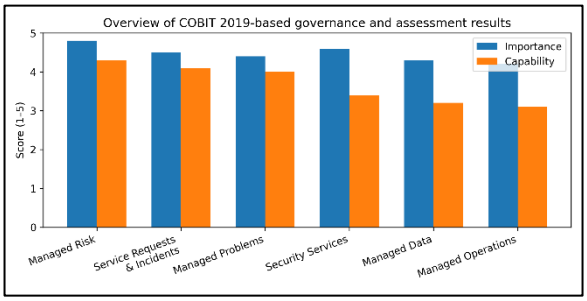

Figure 1. Overview of COBIT 2019-based governance and assessment results.

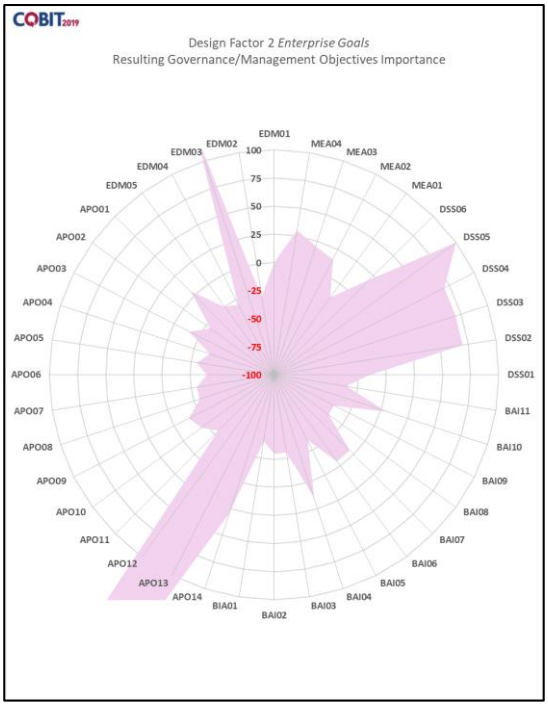

Figure 2. Overview of COBIT 2019-based governance and assessment results.

II. Literature Review

This section of the research is based on reviewing the literature, where the data is extracted from Governance in Higher Education.

A. Governance in Higher Education

The digitalization of higher education has led universities to depend heavily on IT for core academic and administrative processes. Student registration, e-learning platforms, research

collaboration, library services, and financial management all rely on integrated information systems. Effective IT governance is therefore essential to ensure reliability, security, and alignment with institutional goals.

Previous studies emphasize that IT governance in universities must address not only technical controls but also organizational structures, decision rights, and stakeholder engagement. Governance mechanisms such as steering committees, IT policies, service-level agreements, and performance dashboards are widely recommended, but their implementation and maturity vary significantly across institutions, particularly between public and private universities and between large and small institutions.

B. COBIT 2019 Framework

COBIT 2019 builds on earlier versions of COBIT by introducing a flexible design approach centered on governance system components and design factors. The framework is organized into governance objectives (EDM domain) and management objectives (APO, BAI, DSS, MEA domains). Each objective specifies related processes, practices, and metrics and can be tailored based on enterprise strategy, risk profile, and compliance requirements.

Key features relevant to universities include risk optimization, benefit realization, service continuity, information security and data protection, and performance monitoring and compliance. COBIT 2019 also provides a performance management approach based on capability levels, which allows institutions to assess the current state of processes and define realistic target levels that reflect their strategic ambitions and resource constraints.

C. Security, Risk, and Compliance-Driven Governance

Security, risk, and compliance (SRC) have emerged as central drivers of IT governance in universities. Studies highlight the increasing sophistication of cyber threats, the sensitivity of student and research data, and growing regulatory pressure related to privacy, academic integrity, and financial transparency. A security- and risk-centered governance model emphasizes proactive identification of threats, structured risk assessments, and continuous compliance monitoring supported by regular audits and reporting.

Universities must balance openness and collaboration with the need for strong controls. As institutions adopt more cloud-based services, mobile access, and external collaborations, their exposure to cyber risks increases, making a coherent SRC-driven governance framework even more important.

D. Theoretical Framework

The theoretical framework is based on the assumption that Big Data can be used to improve diseases surveillance in health facilities in Nigeria. There are several theories that can be used to explain how Big Data can be used to improve diseases surveillance. One theory is the concept of network theory. Network theory states that nodes in a network are connected to each other. This means that information can flow from one node to another [22]. This theory can be used to explain how information can flow from health facilities to the Nigeria Centre for Disease Control. Another theory is the concept of social network analysis. Social network analysis states that individuals in a social network are connected to each other. This means that information can flow from one individual to another. This theory can be used to explain how information can flow from health facilities to the Nigeria Centre for Disease Control. Moreover, the theoretical framework is based on the assumption that Big Data can be used to improve diseases surveillance in health facilities in Nigeria. This means that the use of Big Data can help to improve the efficiency of diseases surveillance in health facilities in Nigeria.

E. Process Capability and Maturity

Several studies apply COBIT 2019 to assess process capability levels in universities. These works demonstrate that COBIT offers a structured model for evaluating current maturity and

identifying improvement paths. The capability levels provide a common language for communicating the status of governance and management processes to senior leaders, auditors, and technical staff.

However, many assessments focus on a small subset of objectives or treat capability as an end in itself. Fewer studies link capability scores to concrete performance indicators such as downtime, incident rates, or data-loss events. This limits the ability of decision-makers to understand how improvements in governance practices translate into tangible benefits for students, staff, and management.

F. IT Governance Design and Strategic Alignment

Research on IT governance design emphasizes the importance of strategic alignment between IT and institutional goals. The APO01 and APO02 objectives in COBIT 2019 highlight enterprise architecture, portfolio management, and alignment of IT initiatives with enterprise strategy. In universities, this means ensuring that investments in infrastructure, applications, and security controls directly support academic quality, research productivity, and student experience.

Without such alignment, IT initiatives risk becoming isolated projects that consume resources without delivering sustainable value. COBIT 2019 encourages linking governance objectives to enterprise goals and key performance indicators, thus providing a framework for monitoring how IT contributes to teaching, learning, and institutional reputation.

G. Data Governance in Universities

Despite increased attention to cybersecurity, data governance remains a relatively weak area in many institutions. COBIT 2019 stresses the need for data classification, ownership, stewardship, and lifecycle management. In practice, universities often lack clear data owners, consistent retention policies, or enterprise-wide data quality monitoring. Common challenges include fragmented data stores across departments, inconsistent coding schemes, inadequate backup and archiving practices, and limited use of metadata standards. These challenges can undermine the reliability of management information and create hidden risks related to privacy, accreditation, and decision-making.

H. Synthesis and Research Gap

Overall, existing literature acknowledges COBIT 2019 as a suitable framework for IT governance in universities, but empirical studies that apply the full design-factors approach, combine capability assessments with operational KPIs, and focus on risk and continuity in a single integrated model remain limited. This study seeks to fill this gap by offering a case-based, mixed-methods evaluation in the context of a Saudi higher education institution and by demonstrating how capability analysis can be linked with concrete operational performance data.

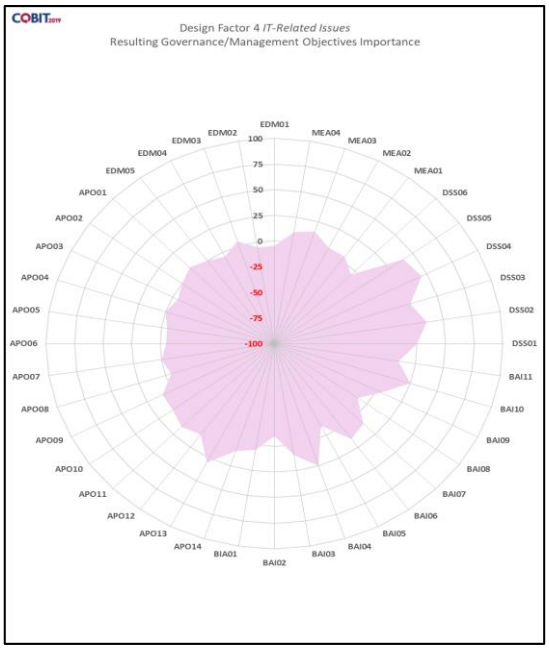

Figure 3. Design factors and high-level governance objectives derived from COBIT 2019.

III. Research Methodology

A. Research Design

A mixed-methods approach was adopted to provide a comprehensive view of IT governance. The research design integrates quantitative data (structured surveys and operational logs) with qualitative data (semi-structured interviews and document analysis). The overall process followed the COBIT 2019 Governance System Design approach, starting from design factor identification and ending with prioritized governance and management objectives.

The mixed-methods design allows both breadth and depth: quantitative data provide measurable indicators of perceived maturity and performance, while qualitative data give insight into the underlying reasons, cultural factors, and institutional constraints that shape IT governance practices.

B. Case Institution and Sample

The study was conducted in a medium-sized private higher education institution in Saudi Arabia with multiple academic programs and a centralized IT department. A total of 250 participants completed the survey, including IT personnel, administrators, faculty members, and decision-makers. This distribution ensured representation from operational, academic, and strategic stakeholders and reflects the diversity of perspectives involved in IT governance.

The selection of a single case institution enables an in-depth examination of context-specific dynamics, but it also means that findings should be interpreted with caution when generalizing to other universities with different sizes, governance models, or national regulations.

C. Data Collection Methods

Interviews were conducted with key stakeholders, including senior management, IT leaders, internal auditors, and quality assurance officers. A structured questionnaire captured the perceived importance of COBIT 2019 design factors, the perceived maturity and effectiveness of selected governance and management objectives, and experience with incidents, data-loss events, and service disruptions.

Institutional policies, IT procedures, risk registers, incident logs, and audit reports were analyzed to triangulate and validate survey and interview data. This combination of sources enhances the reliability of findings and reduces the risk of bias associated with self-reported data.

D. COBIT 2019 Design Factors

The study used the COBIT 2019 Governance System Design Workbook to prioritize objectives based on the following main design factors: enterprise strategy, enterprise goals, risk profile, IT-related issues, threat landscape, compliance requirements, role of IT, sourcing model, IT implementation methods, and technology adoption strategy. Each design factor was rated on importance, and these ratings were used to calculate relative importance scores for COBIT 2019 governance and management objectives.

The use of design factors ensures that the governance system is not applied as a generic

template but is instead customized to the institutional environment, reflecting local risks, priorities, and constraints.

E. Performance Indicators

To connect capability to performance, four KPIs were defined and measured where data were available: downtime minutes for critical systems, mean time to repair (MTTR) for major incidents, SLA attainment for incidents resolved within agreed time, and data-loss frequency representing the number of confirmed data-loss events per year.

These indicators were chosen because they are understandable by both technical and non-technical stakeholders and directly reflect the reliability, responsiveness, and resilience of IT services that support teaching and administration.

F. Data Analysis

Qualitative data were analyzed using thematic analysis, generating themes such as risk awareness, continuity planning, and data stewardship. Quantitative data underwent descriptive statistics and correlation analysis to explore relationships between design factors and governance outcomes. COBIT 2019 capability assessments were mapped to performance KPIs, enabling identification of high-capability high-performance areas and low-capability high-risk areas where improvement is most urgent.

The integration of qualitative and quantitative results was carried out during the interpretation stage, where convergent or divergent evidence was examined to build a coherent explanation of the institution's IT governance strengths and weaknesses.

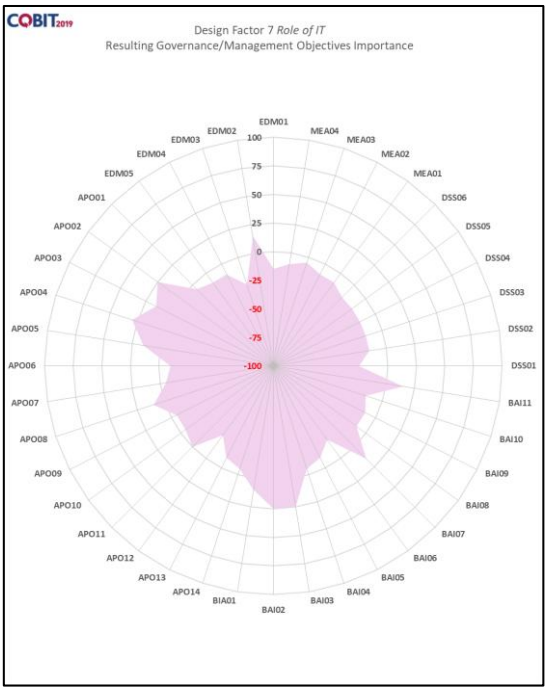

Figure 4. Research methodology flow and resulting capability profiles.

IV. FINDINGS

A. Design Factors and Strategic Priorities

The design factor analysis revealed that the institution's enterprise strategy is strongly oriented toward client service and stability, with lower emphasis on aggressive growth or radical innovation. Enterprise goals related to managed business risk and business-service continuity and availability received the highest importance scores from respondents. This strategic profile explains why governance and management objectives related to continuity and risk received high relative-importance scores in the COBIT 2019 toolkit.

Stakeholders expressed a strong expectation that IT services should be reliable, secure, and responsive to user needs, especially during critical academic periods such as registration and examinations. These expectations drive the focus on risk and continuity objectives in the governance system design.

B. Capability and Performance of Key Processes

The results show a clear pattern: risk-oriented processes and frontline incident handling are relatively strong, while security services, data governance, and operations are weaker and remain below the institution's strategic priorities. Operational data indicate that downtime for critical systems has decreased compared to pre-COBIT baselines but remains above management's expectations in peak periods such as the beginning of the semester and final exams.

Mean time to repair has improved for common incidents but remains high for complex cross-system problems and for issues that require coordination with external vendors. SLA attainment is relatively strong for service requests but inconsistent for security and continuity incidents. Data-loss frequency has decreased, yet several incidents involving partial loss of academic and administrative data were reported in the last 12–18 months, indicating room for strengthening backup and recovery procedures.

C. Risk Profile and Threat Landscape

The risk profile assessment identified particularly high concern for logical attacks such as malware, phishing, and account compromise, as well as software adoption and usage problems and dependence on a small number of key staff. Stakeholders rated the overall threat level as moderate to high, especially regarding cybersecurity and data protection. Interviewees emphasized increased phishing attempts and growing pressure to comply with national data protection requirements.

In addition, the reliance on third-party cloud services for email, collaboration, and some academic applications introduces new forms of risk that are partially outside the institution's direct control. This reinforces the need for a robust governance framework that addresses vendor management, contractual clauses, and shared responsibility models for security and availability.

D. Stakeholder Perceptions

Thematic analysis of interviews revealed several recurring themes: improved awareness of IT risk and governance, process formalization in incident, problem, and change management, persistent gaps in data governance, and resource constraints that make it unrealistic to implement all COBIT objectives at once. Participants emphasized the need for phased implementation and prioritized investments.

Staff members also highlighted cultural and organizational factors, such as resistance to change, limited time for documentation, and competing priorities, as important barriers to fully embedding governance practices into daily operations.

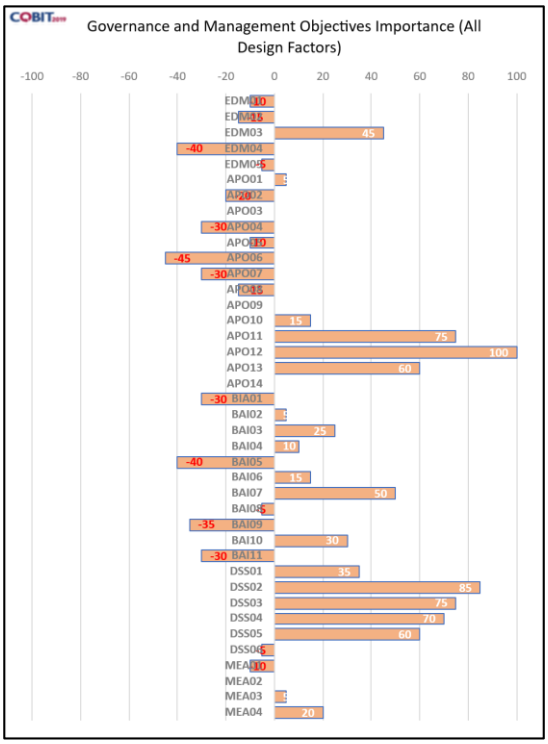

Figure 5. Detailed views of design-factor importance and capability scores for key processes.

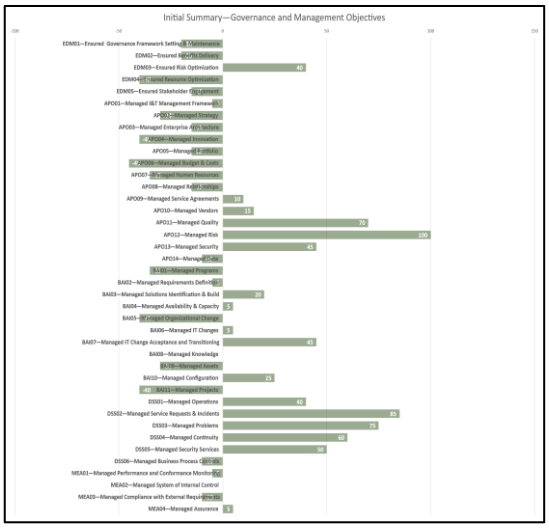

Figure 5. Detailed views of design-factor importance and capability scores for key processes.

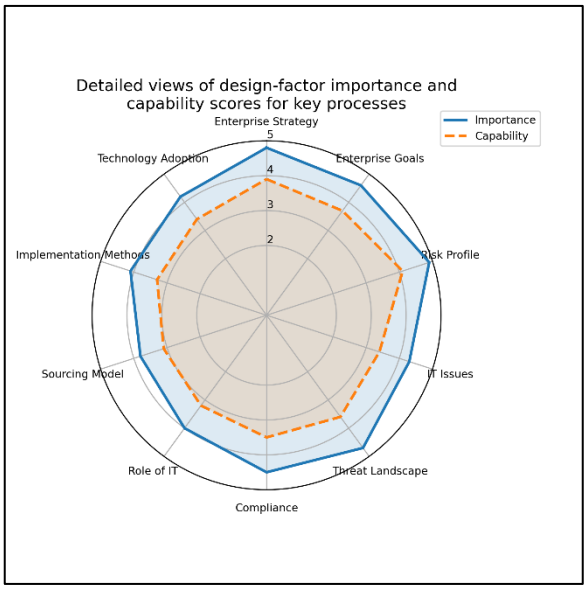

Figure 6. Detailed views of design-factor importance and capability scores for key processes.

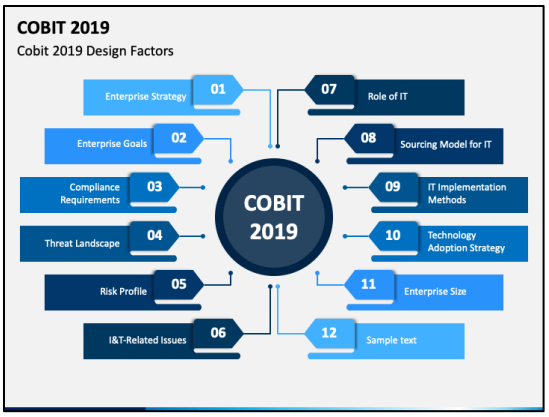

Figure 7. Detailed views of design-factor importance and capability scores for key processes.

V. Discussion

A. COBIT 2019 and Cybersecurity Risk Mitigation

The findings suggest that adopting COBIT 2019 has a positive impact on cybersecurity risk management in the university context. Risk-oriented objectives such as managed risk and managed security services, combined with monitoring and assurance processes, encourage structured identification, assessment, and treatment of IT-related risks. The observed improvements in incident handling, reduction in downtime, and increased risk awareness support the hypothesis that efficient technical structures and formal processes contribute to better risk control.

Nevertheless, the persistence of certain types of incidents and the uneven maturity of security controls indicate that COBIT implementation is an ongoing journey rather than a one-time project. The framework provides direction and structure, but sustained efforts in training, technology upgrades, and policy enforcement are required to realize its full benefits.

B. Continuity, Service Management, and Institutional Resilience

The institution's strategic emphasis on client service and stability translates into high priority for

service management and continuity. Post-implementation results show tangible progress in incident handling and continuity planning, yet they also reveal that continuity capabilities have not fully caught up with expectations. This indicates that governance intent alone is insufficient; universities must translate intent into concrete investments in redundancy, recovery infrastructure, documentation, and periodic testing.

Building institutional resilience requires not only technical solutions such as failover servers and redundant links, but also well-rehearsed procedures, clear communication channels, and defined roles during crises. COBIT 2019 can act as a guide for integrating these elements into a coherent continuity management approach.

C. Data Governance: The Missing Pillar

Despite its central role in information governance, data governance remains relatively weak at the case institution. Fragmented ownership, lack of a unified data catalog, and inconsistent backup and archiving practices contribute to residual data-loss risk. The results suggest that universities should treat data governance as a foundational capability, not a secondary concern, by defining data owners and stewards, establishing classification and retention policies, implementing regular data-quality checks, and integrating data governance metrics into monitoring and assurance activities.

Strengthening data governance would also support other institutional priorities, such as analytics for decision-making, reporting to accreditation bodies, and transparency toward students and stakeholders regarding the use and protection of their data.

D. Integration with ITIL and Other Frameworks

The case institution uses ITIL-inspired practices for incident and service management, while COBIT 2019 provides the overarching governance structure. The findings support the view that COBIT and ITIL are complementary: COBIT 2019 defines what should be governed and measured, while ITIL provides detailed guidance on how to deliver and support services. A hybrid approach can therefore enhance both governance and operational effectiveness, provided that responsibilities and processes are clearly aligned and not duplicated.

In practice, this means mapping COBIT objectives to ITIL processes, ensuring that service catalogues, incident queues, and configuration management databases are used to support governance objectives rather than operating in isolation.

E. Evaluation of Hypotheses

The empirical findings support the first hypothesis: the efficiency of technical structures and formalized processes, assessed through COBIT capability levels, is associated with improved risk management and continuity performance. The second hypothesis is partially supported: COBIT implementation enhances performance in risk and incident domains, but the absence of mature data governance and operations limits the overall institutional benefits.

These results highlight the importance of a balanced implementation strategy that does not neglect foundational areas such as data governance, documentation, and operational procedures while seeking quick wins in risk and compliance domains.

F. Figure 15. Additional analysis charts supporting the discussion section.

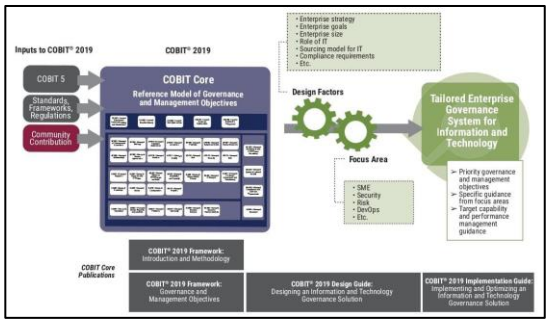

Figure 8. Additional analysis charts supporting the discussion section.

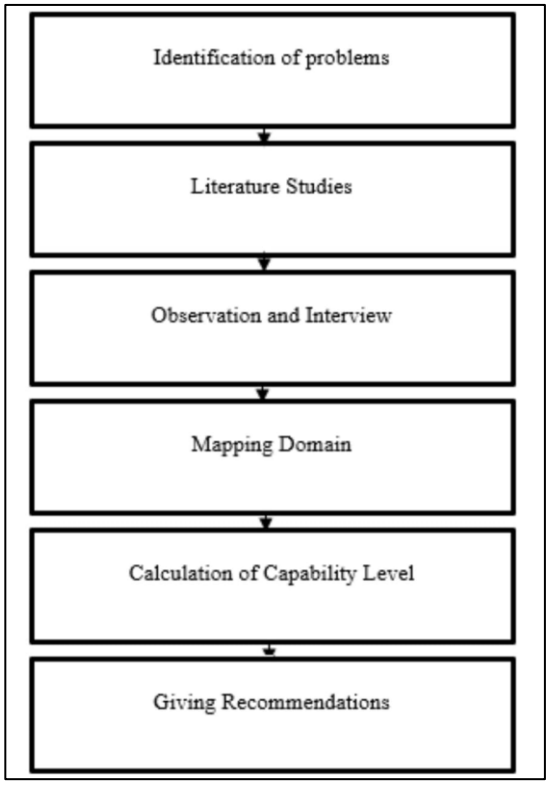

Figure 16. Additional analysis charts supporting the discussion section

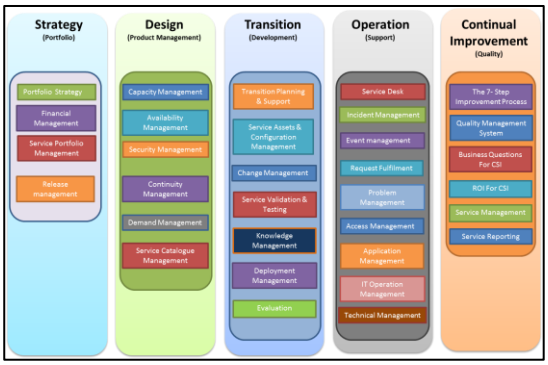

Figure 9. Additional analysis charts supporting the discussion section.

VI. Conclusion and Future Work

This study demonstrates the value of COBIT 2019 as a structured framework for enhancing information governance and risk management in higher education. Using a mixed-methods design, it shows that risk management and incident handling processes can reach high capability and performance levels when aligned with institutional strategy and supported by clear roles and procedures. However, continuity, security services, and data governance require sustained investment and cross-functional collaboration to close the gap between desired and actual performance.

Operational KPIs such as downtime minutes, MTTR, SLA attainment, and data-loss frequency are essential for translating abstract capability levels into tangible performance evidence. Regular measurement and transparent reporting of these indicators can also reinforce accountability and support data-driven decision-making at the executive level.

Future research could conduct longitudinal studies to track capability and performance improvements over several years, compare multiple universities to identify contextual factors that influence COBIT 2019 outcomes, explore the integration of COBIT 2019 with emerging AI-based monitoring tools, and extend the analysis to

academic analytics, research data governance, and student success systems. For practitioners, the key recommendation is to adopt a phased, prioritized implementation of COBIT 2019 with early focus on risk optimization, service continuity, security services, data governance, and continuous monitoring and compliance.

REFERENCES

[1] Abdulrasool, F. E., & Turnbull, S. J. (2020). Exploring security, risk, and compliance-driven IT governance model for universities: Applied research based on the COBIT framework. International Journal of Electronic Banking, 2(3), 237–252. https://doi.org/10.1504/IJEBANK.2020.111438

[2] Abdurrahman, L. (2024). Control self-assessment on information technology business processes as COBIT 2019-based pre-audit activities. International Journal of Knowledge Management in Tourism and Hospitality, 3(3), 185–200. https://doi.org/10.1504/IJKMTH.2024.136327

[3] Amali, L. N., Katili, M. R., & Suhada, S. (2023). Core model of information technology governance system design in local government. TELKOMNIKA (Telecommunication Computing Electronics and Control), 21(4), 750–761. https://doi.org/10.12928/telkomnika.v21i4.24287

[4] Atrinawati, L. H., Ramadhani, E., Fiqar, T. P., Wiranti, Y. T., Abdullah, A. I. N. F., Saputra, H. M. J., & Tandirau, D. B. (2021). Assessment of process capability level in University XYZ based on COBIT 2019. Journal of Physics: Conference Series, 1803(1), 012033.

[5] Fernandez, S., Imanullah, M., Fathoni, M. Y., & Pahrizal, P. (2022). Utilization of the COBIT 2019 framework to identify the level of governance in internet services. Jurnal Infotel, 14(3), 188–195. https://doi.org/10.20895/infotel.v14i3.791

[6] Harits, A., Gernowo, R., & Suseno, D. E. (2022). Adaptation of information systems strategic planning of universities using COBIT 2019 in the post-COVID-19 era. Jurnal Sains dan Teknologi, 11(2), 339–350. https://doi.org/10.23887/jstundiksha.v11i2.48365

[7] Ishlahuddin, A., Handayani, P. W., Hammi, K., & Azzahro, F. (2020). Analysing IT governance maturity level using COBIT 2019 framework: A case study of a small-sized higher education institute. In Proceedings of the IEEE International Conference on Informatics and Computing (IC2IE). https://doi.org/10.1109/IC2IE50715.2020.9274599

[8] Li, Y., & Rong, Y. (2021). Management competency framework for adopting information systems and data governance based on COBIT 2019. Scientific Journal of Economics and Management Research, 3, 1–7. https://www.sjemr.org/download/SJEMR-3-3-1-7.pdf

[9] Oñate-Andino, A., Mauricio, D., Arcos-Medina, G., & Pastor, D. (2018). The application and use of information technology governance at the university level. Advances in Intelligent Systems and Computing, 1028–1038. https://doi.org/10.1007/978-3-030-01174-1_78

[10] Sipayung, A. B., Yunis, R., & Elly, E. (2022). Evaluation of information technology governance at Mikroskil University using COBIT 2019 framework with BAI11 domain. International Journal of Research and Applied Technology, 2(2), 128–143. https://doi.org/10.34010/injuratech.v2i2.8085

[11] Tulus, B. V., & Tanaamah, A. R. (2023). Design of information technology governance in educational institutions using COBIT 2019 framework. Journal of Information Systems and Informatics, 5(1), 31–43. https://doi.org/10.51519/journalisi.v5i1.408

Optional / Supporting References (if needed)

[12] Bagus, P. D., & Lily, W. (2019). Auditing the implementation of information technology governance in a financial services company using COBIT 4.1 framework. International Journal of Open Information Technologies, 7(11), 86–93.

[13] Steuperaert, D. (2019). COBIT 2019: A significant update. EDPACS, 59(1), 14–18. https://doi.org/10.1080/07366981.2019.1578474

[14] Toifur, T., Kusrini, K., & Budi, A. (2022). Evaluation of information technology governance using COBIT 5 and ISO/IEC 38500. Jurnal Online Informatika, 7(1), 17–27. https://doi.org/10.15575/join.v7i1.814

[14] Al Moaiad, Y., Alobed, M., Alsakhnini, M., & Momani, A. M. (2024). Challenges in natural Arabic language processing. Edelweiss Applied Science and Technology, 8(6), 4700-4705.

[15] Al Moaiad, Y., D., Alkhateeb, M., & Alokla, M. (2024). Deep Analysis of Iris Print and Fingerprint for Detecting Drug Addicts. J. Electrical Systems, 20(3), 5639-5644.

[16] Al Moaiad, Y., D., Alkhateeb, M., & Alokla, M. (2024). Enhancing Cybersecurity Practices in Nigerian Government Institutions an Analysis and Framework. J. Electrical Systems, 20(3), 5964-5967.