ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

# "Development of an Integrated Information Security Governance Maturity Assessment Framework for Higher Education Institutions Using COBIT 2019 and ISO/IEC 27001: A Design Science Research Approach"

**Francis R. Abraham; Eduardo R. Yu II**

**AMA University**

**DOI: https://doi.org/10.51583/IJLTEMAS.2026.150600019**

**Received: 17 June 2026; Accepted: 22 June 2026; Published: 03 July 2026**

## ABSTRACT

The adoption of digital technologies, online learning platforms, and electronic services has significantly changed the functioning of higher education institutions. Universities and colleges now rely extensively on digital platforms for teaching, learning, research, and administrative functions. As a result, these institutions manage large quantities of sensitive data, including student records, financial information, research findings, and other vital assets.

In parallel, the rise in cybersecurity threats has underscored the necessity for enhanced information security governance to protect these resources and ensure secure and efficient technology use across campuses. Although established frameworks such as COBIT 2019 and ISO/IEC 27001 offer valuable guidance on governance and information security management, they are often implemented independently. This separation can cause gaps, overlaps, and inconsistencies in governance practices. To address this issue, this study developed an Integrated Information Security Governance Maturity Assessment Framework specifically for Higher Education Institutions by merging the governance principles of COBIT 2019 with the information security management demands of ISO/IEC 27001.

The research employed a Design Science Research (DSR) methodology to develop a framework that is robust in theory and applicable to the higher education sector. This framework was built through a comprehensive analysis of COBIT 2019, ISO/IEC 27001:2022, relevant academic sources, and existing governance maturity models. The resulting framework encompasses five assessment dimensions: Governance and Leadership, Risk and Compliance Management, Security Operations and Control Management, Monitoring and Performance Evaluation, and Continuous Improvement and Governance Optimization.

Additionally, a five-level maturity model was crafted to enable institutions to evaluate their current governance capability and identify areas needing further development. Findings indicate that integrating COBIT 2019 and ISO/IEC 27001 results in a more systematic and thorough approach to information security governance. The framework provides higher education institutions with a practical tool for assessing governance maturity, planning improvement efforts, and enhancing cybersecurity governance. It also lays the groundwork for further implementation, testing, and empirical validation in real university settings.

**Keywords:** Information Security Governance, Cybersecurity Governance, COBIT 2019, ISO/IEC 27001, Governance Maturity, Maturity Assessment Framework, Higher Education Institutions, Design Science Research.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

# INTRODUCTION

## Background of study

The digital revolution of higher education has significantly increased institutional dependence on information systems, cloud services, learning management systems, administrative platforms, and online communication technologies (Bianchi et al., 2021). Universities manage large volumes of sensitive information, including student records, employee details, financial data, examination results, research outputs, and intellectual property. As a result, information security governance has become a strategic concern rather than just a technical responsibility (Merchan-Lima et al., 2020).

Data breaches in higher education are no longer rare occurrences. As universities continue to depend on digital technologies and online services, the potential impact of security incidents has grown more serious. Beyond the loss or exposure of sensitive information, such breaches can harm institutional reputation and weaken the trust that students, faculty, staff, and other stakeholders place in the institution. According to Martin (2016), individuals expect organizations to manage their personal data responsibly based on an implicit social contract. When this expectation is broken, confidence in the institution may decline, leading to concerns about privacy and accountability.

The consequences of data breaches also reach beyond technical and financial effects. Solove and Citron (2018) argued that such incidents can cause feelings of uncertainty, anxiety, and fear among affected individuals, even when immediate harm is not visible. In higher education contexts, where large amounts of personal, academic, and research-related information are stored and processed, these issues become especially significant. Therefore, universities must treat information security not only as a technical necessity but also as a governance duty that helps preserve stakeholder trust, sustain institutional credibility, and maintain a secure learning and working environment.

Cole-Walker (2026) notes that the primary mission of higher education has traditionally been to educate students. Today, that mission has expanded to include information discovery and knowledge transfer. Institutions must fulfill these responsibilities through a range of activities, such as research, extension, health and social services, and human and veterinary medicine. Each of these areas requires a distinct strategic focus and deliberate management. Innovation and adaptation remain essential for long-term sustainability.

Information security governance refers to the policies, processes, and leadership practices that show how an organization protects its information assets while supporting its objectives and managing security risks. Effective governance helps institutions align security efforts with organizational goals, comply with regulations, and maintain stakeholder confidence. As cyber threats continue to rise, universities need to strengthen their governance practices to safeguard critical information and systems (Alsalem et al., 2026).

Globally recognized frameworks such as COBIT 2019 and ISO/IEC 27001 offer structured guidance for information technology governance and information security management. COBIT 2019 focuses on governance objectives, performance management, risk optimization, and value creation (De Haes et al., 2020), while ISO/IEC 27001 outlines requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) (Zúñiga et al., 2025). Although both frameworks are widely used, they are often applied separately, leading to fragmented governance and security management practices.

Recent research has highlighted the importance of integrated governance approaches that combine strategic governance with operational security management. In higher education settings, where organizational structures are often decentralized and stakeholder groups diverse, such integration becomes particularly relevant. However, there is limited research focused on developing a unified maturity assessment framework specifically suited to higher education institutions.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

This study aims to address this gap by presenting an integrated Information Security Governance Maturity Assessment Framework that merges COBIT 2019 governance objectives with ISO/IEC 27001 information security requirements through a Design Science Research approach.

## LITERATURE REVIEW

The theoretical and literature supporting the development of an Integrated Information Security Governance Maturity Assessment Framework for Higher Education Institutions. The review examines information security governance, cybersecurity challenges in higher education, governance maturity models, COBIT 2019, ISO/IEC 27001, Design Science Research, and existing framework integration studies. This establishes the scholarly foundation for the proposed framework and identifies gaps that justify the present study.

Information security governance has evolved from technical concern into a strategic organizational function. It includes the structures, processes, leadership mechanisms, and policies used to direct and control information security activities. Effective governance ensures that security initiatives support institutional objectives while balancing risks and resource utilization.

The literature on cybersecurity and data breaches has gradually expanded beyond technical and compliance-related concerns to include the impact of security incidents on stakeholders. Earlier studies viewed data breaches as failures of information security controls, policies, or regulatory compliance, with most attention given to prevention, detection, and response mechanisms. While these technical aspects remain important, recent research indicates that the consequences of cybersecurity incidents extend beyond technology and can influence how stakeholders perceive an institution's ability to govern and protect information assets.

Studies have shown that cybersecurity incidents often generate emotional responses among affected individuals, including fear, anxiety, frustration, anger, and loss of trust. Budimir et al. (2021) found that individuals commonly experience negative emotional reactions when faced with cybersecurity breach situations. Similarly, Sears and Cunningham (2024) reported that data breach experiences can result in varying levels of psychological stress and concern among affected individuals. These findings suggest that the impact of security incidents is not limited to operational disruption or financial loss but also affects stakeholder confidence and institutional reputation.

In the context of higher education, where institutions manage sensitive student, employee, financial, and research information, stakeholder trust is an important indicator of effective information security governance. The ability of an institution to prevent, manage, and respond to cybersecurity incidents reflects the maturity of its governance practices. Therefore, information security governance should not only focus on technical controls but also on building accountability, transparency, and stakeholder confidence. This perspective supports the need for governance maturity assessment frameworks that can help higher education institutions evaluate their governance capability, identify improvement opportunities, and strengthen their overall cybersecurity posture. Thus, the development of an Integrated Information Security Governance Maturity Assessment Framework using COBIT 2019 and ISO/IEC 27001 provides a structured approach for assessing governance maturity and supporting continuous improvement in information security governance.

AlGhamdi and Win (2020) emphasized that information security governance requires strategic alignment, risk management, accountability, performance measurement, and compliance management. Governance offers executive oversight and ensures that information security contributes to organizational value creation.

In higher education institutions, governance becomes increasingly complex because of decentralized organizational structures, diverse stakeholder groups, academic freedom requirements, and extensive digital infrastructures. Bianchi et al. (2021) argued that governance mechanisms in universities must accommodate both institutional autonomy and regulatory requirements. Consequently, governance frameworks must provide flexibility while maintaining security accountability.

Higher education institutions have become increasingly attractive targets for cybercriminals because of the large amount of valuable information they manage. Universities and colleges store sensitive data such as student

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

records, employee information, financial documents, research outputs, and intellectual property. At the same time, academic institutions encourage openness, collaboration, knowledge sharing, and broad access to technology resources. While these characteristics support learning and research, they can also create additional cybersecurity challenges and increase exposure to cyber threats.

According to Ulven and Wangen (2021), universities are particularly vulnerable to cyberattacks because of their complex and distributed information technology environments, as well as their large and diverse user populations. Likewise, Fouad (2021) reported that higher education institutions continue to experience growing numbers of phishing attacks, ransomware incidents, and unauthorized access attempts. These threats can disrupt academic operations, compromise sensitive information, and damage institutional reputation.

Recent literature suggests that cybersecurity should not be treated solely as a technical concern. Cheng and Wang (2022) argued that the effectiveness of cybersecurity programs is strongly influenced by governance structures, leadership commitment, and organizational culture. Effective information security governance enables institutions to identify and manage risks proactively, allocate resources more effectively, establish accountability, and support the development of a strong security culture across the organization.

Maturity models provide organizations with mechanisms for evaluating current capabilities and identifying opportunities for improvement. These models define progressive levels of organizational development, ranging from initial and ad hoc practices to optimized and continuously improving processes.

Aliyu et al. (2020) proposed a cybersecurity maturity assessment framework for higher education institutions that integrates governance, technology, and organizational dimensions. Their findings showed that maturity assessments can support strategic planning and resource prioritization.

According to Tocto-Cano et al. (2020), many maturity models remain fragmented and focus on isolated aspects of governance or security management. As a result, organizations often struggle to obtain a comprehensive view of cybersecurity readiness. This limitation highlights the need for integrated maturity assessment frameworks that combine governance and operational security perspectives.

COBIT 2019 is a globally recognized framework developed by ISACA for enterprise governance and management of information and technology. The framework provides principles, objectives, performance management mechanisms, and governance structures that help organizations align information technology initiatives with business goals.

COBIT 2019 distinguishes governance from management functions and introduces governance objectives that focus on value creation, risk optimization, and resource optimization. Governance objectives are supported by management objectives that address planning, implementation, service delivery, and performance monitoring.

Key governance and management objectives relevant to information security include EDM03 (Ensure Risk Optimization), APO13 (Manage Security), DSS05 (Manage Security Services), and MEA01 (Monitor, Evaluate, and Assess Performance and Conformance). These domains provide a solid foundation for assessing information security governance maturity.

According to ISACA (2019), COBIT 2019 enables organizations to evaluate governance effectiveness through capability and maturity assessments. Therefore, it serves as a suitable governance component for the proposed integrated framework.

ISO/IEC 27001 is the internationally recognized standard for Information Security Management Systems (ISMS). The standard provides requirements for establishing, implementing, maintaining, and continually improving information security management processes.

The framework is organized around the Plan-Do-Check-Act (PDCA) improvement cycle and emphasizes risk-based decision making. Clauses related to leadership, planning, support, operation, performance evaluation, and improvement collectively establish a structured approach to information security management.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Culot et al. (2023) noted that ISO/IEC 27001 has become one of the most widely adopted information security standards globally because of its emphasis on continuous improvement and risk management. The standard enables organizations to systematically identify risks, implement controls, and monitor performance.

Although ISO/IEC 27001 provides extensive guidance for operational security management, it does not offer the same level of governance-oriented assessment available in COBIT 2019. This distinction highlights the complementary relationship between both frameworks.

Design Science Research (DSR) is a problem-solving research methodology focused on the creation and evaluation of innovative artifacts. Hevner et al. (2004) defined DSR as a research paradigm that seeks to generate practical and theoretical contributions through artifact development.

Peffers et al. (2007) proposed a six-stage DSR methodology consisting of problem identification, objective definition, design and development, demonstration, evaluation, and communication. DSR has become widely used in information systems research because it supports framework development, model construction, and process innovation.

The current study adopts DSR because its primary objective is to develop an integrated maturity assessment framework rather than measure existing organizational performance. DSR provides a rigorous and systematic approach for framework construction and validation.

Several researchers have examined integration among governance, risk management, and cybersecurity frameworks. Previous studies have combined COBIT with ISO/IEC 27001, ITIL, NIST, and other governance models to improve organizational cybersecurity capabilities. Research indicates that integrated frameworks provide greater organizational visibility, reduce duplication of controls, and strengthen governance alignment. However, most existing integration studies focus on corporate environments rather than higher education institutions.

Furthermore, many studies concentrate on implementation guidance rather than maturity assessment. Consequently, limited research exists regarding integrated maturity models specifically designed for universities and colleges. The present study addresses this gap by proposing a framework that combines governance objectives and security management requirements within a maturity assessment context.

**Theoretical Framework**

This study is founded on three theoretical bases: Governance Theory, Information Security Management System Theory, and Maturity Model Theory.

Governance Theory offers a framework for organizational oversight, responsibility, and strategic alignment. COBIT 2019 applies governance principles using specific objectives and performance management tools.

Information Security Management System Theory facilitates the systematic management of information security through risk-oriented processes, policies, controls, and continuous improvements. ISO/IEC 27001 implements these concepts through established management requirements.

Maturity Model Theory serves as the foundation for assessing organizational capability and process development, positing that organizational practices evolve through distinct stages, enabling a structured approach to assessment and improvement planning.

The combination of these theories supports the creation of a comprehensive information security governance maturity assessment framework.

**Conceptual Framework**

The conceptual framework depicted in Figure 1 employs an Input–Process–Output model.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

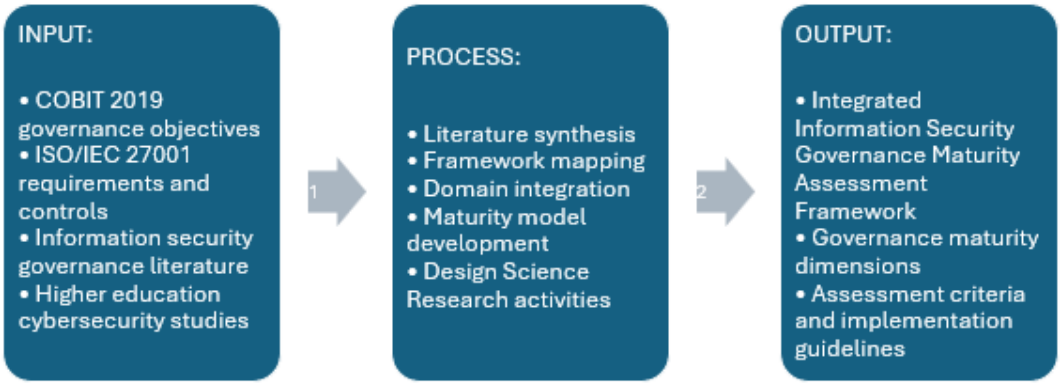
1. Inputs consist of COBIT 2019 governance objectives, ISO/IEC 27001 requirements, cybersecurity governance literature, and governance requirements specific to higher education.

2. The process includes literature review, framework mapping, domain integration, maturity model development, and activities related to Design Science Research.

3. Outputs result in the proposed Integrated Information Security Governance Maturity Assessment Framework, alongside maturity dimensions, assessment criteria, and implementation guidelines.

This framework serves as the conceptual foundation for developing a comprehensive governance maturity assessment model for higher education institutions.

**Figure 1.** The Input-Process-Output Conceptual Framework.




## Synthesis of Literature and Research Gap

Literature indicates that information security governance is crucial for organizational sustainability, cybersecurity resilience, and regulatory compliance, emphasizing the role of governance structures, risk management practices, leadership engagement, and continuous improvement.

Current research highlights a growing focus on cybersecurity governance and maturity assessment but identifies several gaps. Primarily, studies often prioritize cybersecurity controls rather than governance maturity. Additionally, COBIT and ISO/IEC 27001 are typically applied independently despite their complementary roles. Furthermore, few studies offer an integrated maturity assessment framework tailored to the unique context of higher education institutions. Lastly, limited research uses Design Science Research to develop frameworks for information security governance within academic environments (Sengik et al., 2022).

These gaps emphasize the necessity to develop an Integrated Information Security Governance Maturity Assessment Framework that combines COBIT 2019 and ISO/IEC 27001 in a higher education context.

## Problem Statement

Higher education institutions are increasingly reliant on digital technologies for academic and administrative functions. Despite the availability of widely recognized frameworks like COBIT 2019 and ISO/IEC 27001, institutions often face challenges in assessing information security governance maturity comprehensively and systematically. Current methods frequently focus on either governance objectives or security controls, lacking a unified perspective.

The absence of an integrated framework may lead to fragmented assessments, inconsistent governance practices, and limited insights into institutional security capabilities. Therefore, it is essential to develop a comprehensive information security governance maturity assessment framework that incorporates both COBIT 2019 and ISO/IEC 27001 with an application to higher education institutions.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

## Research Questions

### Main Research Question:

How can COBIT 2019 and ISO/IEC 27001 be combined to create an Information Security Governance Maturity Assessment Framework for Higher Education Institutions?

### Sub-Questions:

1. What governance components exist within COBIT 2019?

2. What information security requirements are outlined by ISO/IEC 27001?

3. How can COBIT 2019 and ISO/IEC 27001 be aligned and integrated?

4. What maturity dimensions can result from this integration?

5. How can the proposed framework facilitate governance assessment in higher education?

## Research Objectives

### General Objective:

To construct an Integrated Information Security Governance Maturity Assessment Framework for Higher Education Institutions using COBIT 2019 and ISO/IEC 27001.

### Specific Objectives:

1. Evaluate relevant governance objectives within COBIT 2019.
2. Investigate information security management conditions within ISO/IEC 27001.
3. Determine alignment areas between the two frameworks.
4. Develop an integrated maturity assessment framework.
5. Provide implementation guidelines for higher education institutions.

## Significance of Study

- Academic Significance: This study enriches the information security governance literature by introducing an integrated framework that merges governance and security management views.
- Practical Significance: The framework could assist university leaders, IT managers, and policymakers in assessing governance maturity and identifying opportunities for improvement.
- Institutional Significance: Higher education institutions can apply the framework to enhance cybersecurity, governance, compliance, and risk management.
- Policy Significance: The framework can underpin national digital transformation efforts and cybersecurity strategies by fostering improved governance practices.

## Scope and Delimitations

The study's focus is on developing a conceptual and theoretical framework that integrates COBIT 2019 and ISO/IEC 27001, excluding surveys, interviews, case studies, or organizational data collection. The framework is designed specifically for higher education institutions, centering on governance maturity assessment rather than technical security testing or implementation evaluation.

## Definition of Terms

1. COBIT 2019 – A framework for enterprise governance and management developed by ISACA.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

2. ISO/IEC 27001 – An international standard outlining requirements for information security management systems.
3. Information Security Governance – The framework through which organizations direct and manage information security activities.
4. Maturity Assessment – A structured process to determine the capability and effectiveness of organizational practices.
5. Higher Education Institution – An organization that provides tertiary education, research, and academic services.
6. Design Science Research – A research methodology focused on the creation and evaluation of innovative artifacts intended to solve identified problems.

## METHODOLOGY

This study utilized the Design Science Research (DSR) methodology as defined by Peffers et al. (2007). The DSR approach was selected because the study's primary aim was to create a functional artifact, a comprehensive Integrated Information Security Governance Maturity Assessment Framework for Higher Education Institutions, rather than examine an existing phenomenon. DSR is widely acknowledged as an appropriate methodology for crafting and assessing fresh solutions to challenges in organizational and information systems.

The framework was developed through an extensive examination and analysis of pertinent literature, international standards, and governance frameworks, with a keen focus on COBIT 2019 and ISO/IEC 27001:2022 due to their recognized importance in information security governance and management. Additional academic sources, governance maturity models, and studies on cybersecurity in higher education were also reviewed to identify common governance dimensions, best practices, and assessment requirements.

Adhering to the Design Science Research process, the study initially pinpointed the issue of disjointed information security governance assessment techniques within higher education institutions. Current frameworks often treat governance and security management as isolation, which results in limited organizational understanding and inconsistent evaluation outcomes.

To address this, a conceptual framework was created by merging the governance principles of COBIT 2019 with the information security management requirements of ISO/IEC 27001. The framework encompasses five governance assessment dimensions and a five-level maturity model, developed to assess governance capabilities and promote continuous progress.

The proposed artifact was then subjected to theoretical validation by comparing it with existing governance and maturity assessment frameworks from the literature, ensuring that it is conceptually robust, aligned with recognized standards, and suitable for the higher education environment.

Through the application of the Design Science Research methodology, this study delivers an organized and systematic approach to framework development, contributing both theoretical and practical insights to information security governance. The proposed framework lays a foundation for future empirical validation and deployment in higher education institutions.

### Research Paradigm

The study is anchored in the pragmatist research paradigm, prioritizing problem-solving, and the practical application of knowledge. Pragmatism advocates for the development of innovative solutions to real-world organizational issues. In the field of information systems research, pragmatism complements Design Science Research, as both prioritize the creation of useful artifacts that enhance theory and practice. The purpose of the study is to construct a theoretically sound and relevant framework that can support information security governance maturity assessments within higher education institutions, rather than measure organizational performance or evaluate causal relationships.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

**Research Design**

The study adopts the Design Science Research (DSR) methodology. DSR has gained widespread acceptance in information systems research as it facilitates the creation of artifacts that address identified organizational issues. Hevner et al. (2004) states that DSR is centered on the development and assessment of innovative artifacts, such as models, methods, frameworks, and systems. Peffers et al. (2007) further outlined a structured six-stage process to guide artifact development and validation. The artifact developed in this study is an Integrated Information Security Governance Maturity Assessment Framework that merges governance objectives from COBIT 2019 with information security management requirements from ISO/IEC 27001.

**Design Science Research Process**

The Design Science Research (DSR) process as proposed by Ken Peffers et al. (2007) comprises six interconnected phases (Table 1). The first phase, Problem Identification and Motivation, sets the issue that needs to be addressed and explains its significance. The second phase, Define the Objectives for a Solution, establishes what the proposed solution should achieve based on the problem and existing knowledge. The third phase, Design and Development, involves creating artifacts such as a framework, model, method, or system. The fourth phase, Demonstration, illustrates how the artifact can be applied to resolve the identified issue in a real or simulated setting. The fifth phase, Evaluation, determines how well the artifact meets its objectives and identifies areas for improvement. Lastly, the sixth phase, Communication, involves disseminating the research process, findings, and contributions to academic and professional audiences. Collectively, these six phases offer a systematic approach for crafting and validating practical solutions to real-world problems.

**Table 1**. The six phases of Design Science Research.

| Phase No. | Phases | Description |
|---|---|---|
| **Phase 1:** | Problem Identification and Motivation | The study identifies the lack of integrated information security governance maturity assessment frameworks specifically designed for higher education institutions. |
| **Phase 2:** | Define Objectives for a Solution | The objective is to develop a framework that integrates governance and information security management principles into a comprehensive maturity assessment model. |
| **Phase 3:** | Design and Development | The framework is developed through systematic literature review, framework mapping, and maturity model construction. |
| **Phase 4:** | Demonstration | The proposed framework is conceptually demonstrated through framework architecture and governance domain mapping. |
| **Phase 5:** | Evaluation | The framework is evaluated through theoretical validation and comparative analysis against existing frameworks. |
| **Phase 6:** | Communication | The results are documented and communicated through academic dissemination and scholarly publication. |

**Sources of Data**

The study did not require primary data collection since there are no human participants involved. Instead, it relied exclusively on documentary sources, which include:

- Publications on the COBIT 2019 Framework
- Documentation for ISO/IEC 27001:2022 Standard
- Publications by ISACA on Governance
- Publications by the International Standards Organization

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

- Peer-reviewed journal articles
- Studies on cybersecurity governance
- Literature on cybersecurity in higher education
- Research on information systems governance

These resources provide the theoretical and practical foundations essential for framework development.

**Literature Selection Procedure**

The study employs a systematic process for selecting literature to ensure quality and relevance. Literature was chosen based on the following criteria:

Inclusion Criteria:

- Peer-reviewed publications
- Studies published between 2020 and 2026
- Research on information security governance
- Studies on cybersecurity in higher education
- Research related to COBIT
- Research related to ISO/IEC 27001
- Research on governance maturity assessment

Exclusion Criteria:

- Non-academic publications
- Duplicate studies
- Non-English literature
- Studies that do not pertain to governance or maturity assessment.

This selection process ensures that the proposed framework is grounded in contemporary scholarly evidence.

## FRAMEWORK MAPPING METHODOLOGY

Framework mapping is the study's central development activity. It involves methodically identifying and linking the governance objectives of COBIT 2019 with the information security controls and requirements of ISO/IEC 27001. By examining the complementary nature of these frameworks, the study creates an integrated structure that merges COBIT 2019's governance and management perspective with ISO/IEC 27001's approach to security control and risk management. This mapping procedure forms the foundation for developing a unified information security governance maturity assessment framework for higher education institutions. The mapping methodology, as illustrated in Table 2, provides a structured approach to integrating governance and security management perspectives.

**Table 2**. The framework mapping process.

| Step No. | Process | Description |
|---|---|---|
| **Step 1** | Identification of Relevant COBIT Domains | Relevant governance and management objectives are selected based on their relationship to information security governance. |
| **Step 2** | Identification of Relevant ISO/IEC 27001 Components | Relevant clauses and Annex A controls are identified based on governance and security management relevance. |
| **Step 3** | Cross-Mapping Analysis | Corresponding governance and security management elements are analyzed and aligned. |

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

| | | |
|---|---|---|
| **Step 4** | Domain Consolidation | Overlapping concepts are consolidated into integrated governance dimensions. |
| **Step 5** | Maturity Dimension Development | The integrated domains are translated into maturity assessment criteria and maturity levels. |

**Framework Development Procedure**

The framework development follows an iterative process. The initial governance domains are extracted from COBIT 2019's governance objectives, while operational security domains are derived from ISO/IEC 27001's requirements. The development involves:

- Governance domain identification
- Security management domain identification
- Domain integration
- Maturity level construction
- Development of assessment criteria
- Framework architecture design
- Development of implementation guidelines

The resulting framework combines strategic governance oversight with operational security management requirements.

**Proposed Maturity Model Development**

The maturity model proposed in this study is structured around five levels, as outlined in Table 3, adapted from established maturity assessment approaches. These levels characterize the progression of an institution's information security governance practices from basic or informal processes towards structured, managed, and continuously refined practices. The model provides a systematic method for evaluating the status of information security governance and aids institutions in pinpointing areas for improvement and planning their progress towards higher maturity levels.

**Table 3.** The proposed maturity model provides a structured mechanism for assessing governance capability and organizational readiness.

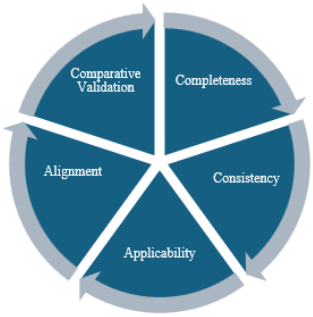
| Level No. | Process | Description |
|---|---|---|
| **Level 1** | Initial | Processes are informal, reactive, and undocumented. |
| **Level 2** | Repeatable | Basic governance practices exist and can be repeated. |
| **Level 3** | Defined | Processes are formally documented and standardized. |
| **Level 4** | Managed | Performance measurement and monitoring mechanisms are implemented. |
| **Level 5** | Optimized | Continuous improvement and governance excellence are institutionalized. |

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

## Framework Validation Strategy

As the study does not involve empirical data collection, validation is focused on theoretical rigor and conceptual consistency. Framework validation (Figure 2) emphasizes theoretical integrity and internal coherence over empirical testing. The validation process entails reviewing the developed framework against established concepts, principles, and best practices documented in the literature related to COBIT 2019 and ISO/IEC 27001. This ensures that the mapped components are logically aligned, internally coherent, and capable of supporting the intended information security governance maturity assessment for higher education institutions. This approach helps establish the theoretical credibility and reliability of the framework.

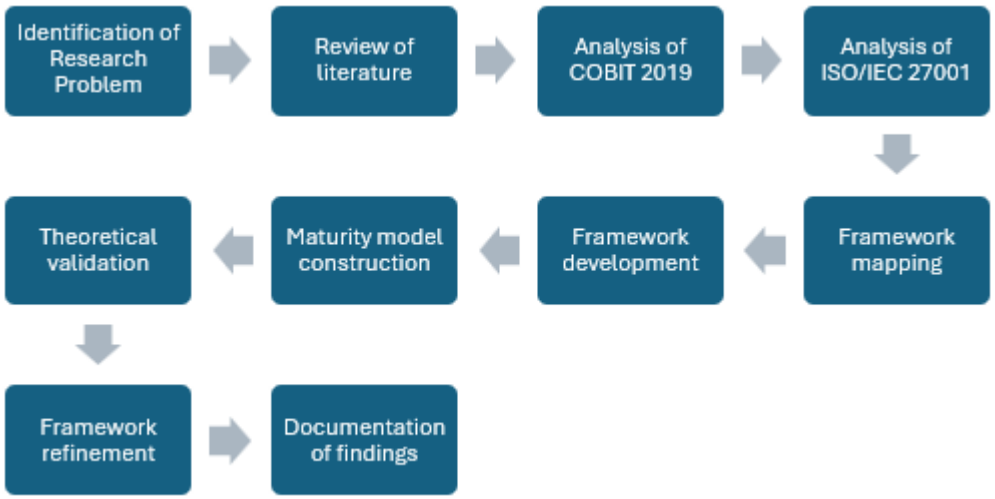
**Figure 2.** The framework is evaluated using the following criteria:




## Research Workflow

The overall research workflow (Figure 3) follows a step-by-step sequence to systematically develop the proposed framework. It begins by identifying the research problem, followed by reviewing relevant literature and analyzing the COBIT 2019 and ISO/IEC 27001 frameworks. The study then maps the interconnections between the two frameworks, develops the integrated governance framework, and constructs the maturity model. Subsequently, the framework undergoes theoretical validation and refinement before the findings are documented. This structured workflow ensures that the framework is developed logically and rigorously, in line with the Design Science Research principles. The workflow ensures systematic progression from problem identification to artifact development.

**Figure 3.** The overall research workflow follows a sequential process.




## Ethical Considerations

The study follows standard academic and research ethics principles. Since no human participants are involved, the concerns related to informed consent, confidentiality, anonymity, and participant protection do not apply. Nonetheless, the study maintains ethical integrity through:

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

- Proper citation of all sources
- Accurate representation of literature
- Avoidance of plagiarism
- Transparent research practices
- Objective framework development

These measures ensure the research's credibility and trustworthiness.

# RESULTS

The development of the Integrated Information Security Governance Maturity study's findings suggests that using IT Service Management (ITSM) frameworks can greatly enhance organizational agility in educational institutions. Literature reviews indicate that institutions effectively implementing ITIL and COBIT often benefit from more standardized processes, improved risk management, and better alignment of IT services with institutional goals. Such enhancements enable universities to adapt more efficiently to changing educational demands, technological advancements, and external pressures (Shivashankarappa et al., 2012).

Integrating ITIL and COBIT ensures a balance between operational efficiency and governance control. ITIL is focused on service quality, continuous improvement, and customer satisfaction, while COBIT emphasizes governance, accountability, and risk management. Combined, these frameworks establish an environment that nurtures both stability and flexibility. Mora et al. (2021) assert that incorporating agile principles into IT service management boosts organizational responsiveness and continuous improvement, while Alkhaldi et al. (2017) argue that effective governance and risk management fortify organizational learning and performance.

Consequently, institutions might experience expedited decision-making, enhanced service delivery, quicker recovery from disruptions, and better support for innovation. The study also highlights the need for leadership commitment and organizational culture to realize ITSM benefits. Despite having governance frameworks, their success relies on leaders and staff being open to change, collaboration, and continuous improvement. Institutions fostering knowledge sharing, innovation, and accountability are more likely to cultivate a culture of agility and resilience.

These findings align with earlier studies recognizing leadership support and organizational readiness as crucial for successful ITSM adoption (Shivashankarappa et al., 2012). Thus, the study supports the notion that ITSM frameworks are not just operational tools but strategic enablers of organizational agility. By combining governance, risk management, and service management practices, academic institutions can enhance their ability to adapt to fast-changing environments while maintaining service quality and institutional performance.

This research contributes valuable insights to IT governance literature and offers practical guidance for university administrators, policymakers, and IT leaders aiming to boost organizational agility in higher education (Winniford et al., 2009).

### Analysis of COBIT 2019 Governance Components

Framework development commenced by examining COBIT 2019 governance and management goals pertinent to information security governance. COBIT 2019 was selected for its comprehensive governance mechanisms that emphasize value creation, risk optimization, resource optimization, and performance measurement (ISACA, 2019).

The analysis identified governance domains related to information security, such as EDM03 (Ensure Risk Optimization), APO13 (Manage Security), DSS05 (Manage Security Services), and MEA01 (Monitor, Evaluate, and Assess Performance and Conformance). These domains collectively address leadership oversight, governance accountability, security management, operational controls, and ongoing monitoring. COBIT 2019's governance perspective lays the strategic foundation for the proposed framework.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

## Analysis of ISO/IEC 27001 Information Security Requirements

The following stage focused on analyzing ISO/IEC 27001:2022 requirements and controls, given its status as an internationally recognized standard for Information Security Management Systems (ISMS). The analysis targeted Clauses 5 through 10, covering leadership, planning, support, operation, performance evaluation, and continual improvement. Additionally, selected Annex A controls were examined to pinpoint operational security management requirements. The results show that ISO/IEC 27001 offers detailed guidance on risk management, access control, security awareness, incident management, monitoring, and continuous improvement. These operational needs complement COBIT 2019's governance orientation.

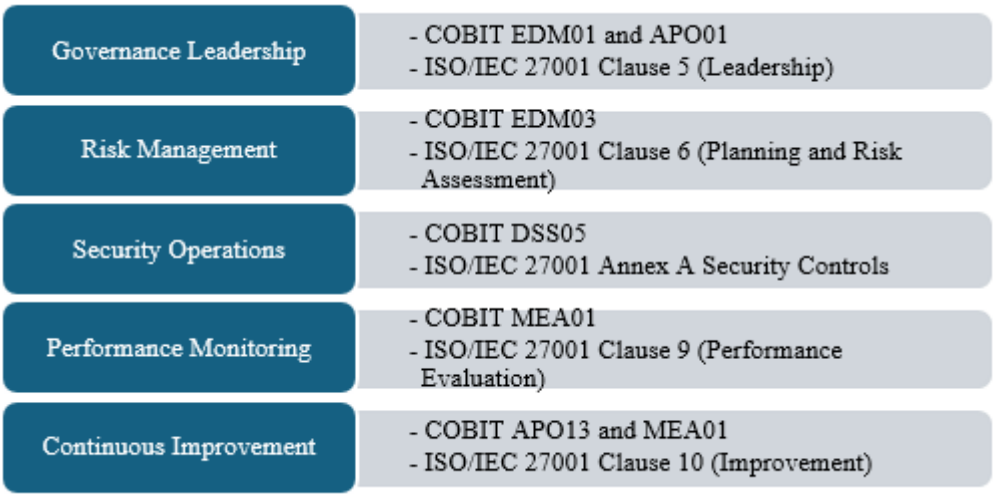
## COBIT 2019 and ISO/IEC 27001 Mapping Results

The cross-framework mapping process, depicted in Figure 4, identified the links between COBIT 2019's governance objectives and ISO/IEC 27001's information security management requirements. The analysis revealed that both frameworks complement each other and share several common elements. COBIT 2019 offers strategic governance and direction, while ISO/IEC 27001 actualizes these objectives into actionable security policies, processes, and controls.

By aligning both frameworks' strengths, the integrated model provides a more comprehensive approach to information security governance and maturity assessment in higher education institutions.

The analysis demonstrated significant overlaps, with COBIT offering strategic direction and ISO/IEC 27001 operationalizing governance goals through management practices and security controls. Thus, the mapping results verified that both frameworks possess complementary traits suitable for integration.

**Figure 4.** Major mapping relationships.




## Development of the Integrated Governance Framework

Based on the mapping outcomes, an integrated governance framework was established, combining strategic governance principles with operational security management needs. It includes five key governance dimensions:

1. Governance and Leadership
2. Risk and Compliance Management
3. Security Operations and Control Management
4. Monitoring and Performance Evaluation
5. Continuous Improvement and Governance Optimization

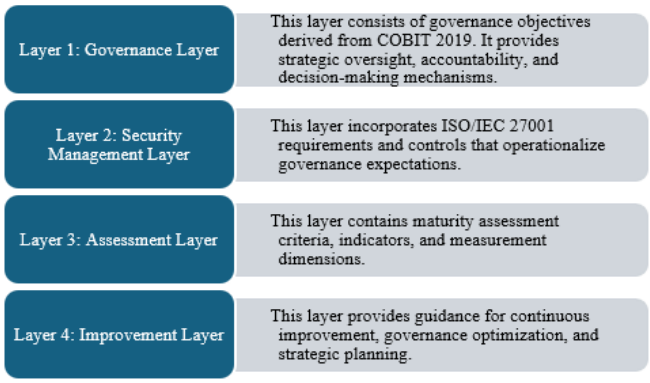
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

These dimensions represent the principal governance domains necessary for a thorough information security governance maturity assessment within higher education. Each dimension encompasses assessment criteria derived from COBIT objectives and ISO/IEC 27001 requirements.

**Proposed Framework Architecture**

The proposed framework architecture consists of four interconnected layers (Figure 5) that collectively support information security governance. The initial layer concentrates on governance and strategic direction, followed by a security management layer encompassing policies and operational controls. The third layer features maturity assessment components for evaluating governance capabilities, and the last layer stresses continuous improvement and the implementation of recommendations. By integrating these layers, the framework offers a structured method for assessing and enhancing information security governance in higher education. The layered design ensures alignment between governance, management, assessment, and improvement activities.

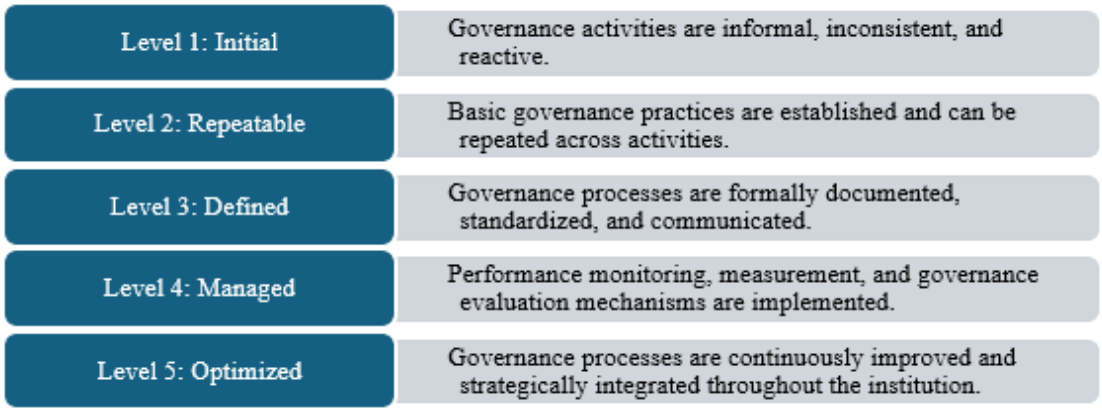
**Figure 5.** The proposed framework architecture.




**Developing the Maturity Model**

The maturity model (Figure 6) aims to provide a structured approach for assessing the capability of an institution's information security governance practices. It employs five recognized maturity levels from governance and process assessment frameworks, allowing organizations to assess their current maturity and identify areas needing improvement. This approach aids in institutions in recognizing their strengths, addressing governance gaps, and planning for the continuous enhancement of their information security governance practices.

**Figure 6.** The maturity levels support organizational benchmarking and continuous improvement planning.




**Proposed Governance Assessment Dimensions**

The proposed framework (Figure 7) evaluates information security governance through five key assessment dimensions. These include Governance and Leadership, which focuses on management commitment and

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

strategic direction; Risk and Compliance Management, which addresses the identification and management of security risks and regulatory requirements; Security Operations, which examines the effectiveness of security controls and operational practices; Performance Evaluation, which measures monitoring, reporting, and governance performance; and Continuous Improvement, which emphasizes organizational learning, corrective actions, and ongoing enhancement of governance processes. Together, these dimensions provide a comprehensive basis for assessing and improving information security governance maturity in higher education institutions.

**Figure 7.** The framework proposes five assessment dimensions.


These dimensions provide comprehensive coverage of governance and security management requirements.

1. Governance and Leadership: Evaluates executive commitment, governance structures, policies, and strategic alignment.
2. Risk and Compliance Management: Assesses risk identification, treatment, monitoring, and regulatory compliance activities.
3. Security Operations: Evaluates operational controls, access management, incident response, and security services.
4. Performance Evaluation: Measures monitoring activities, governance reviews, performance indicators, and reporting mechanisms.

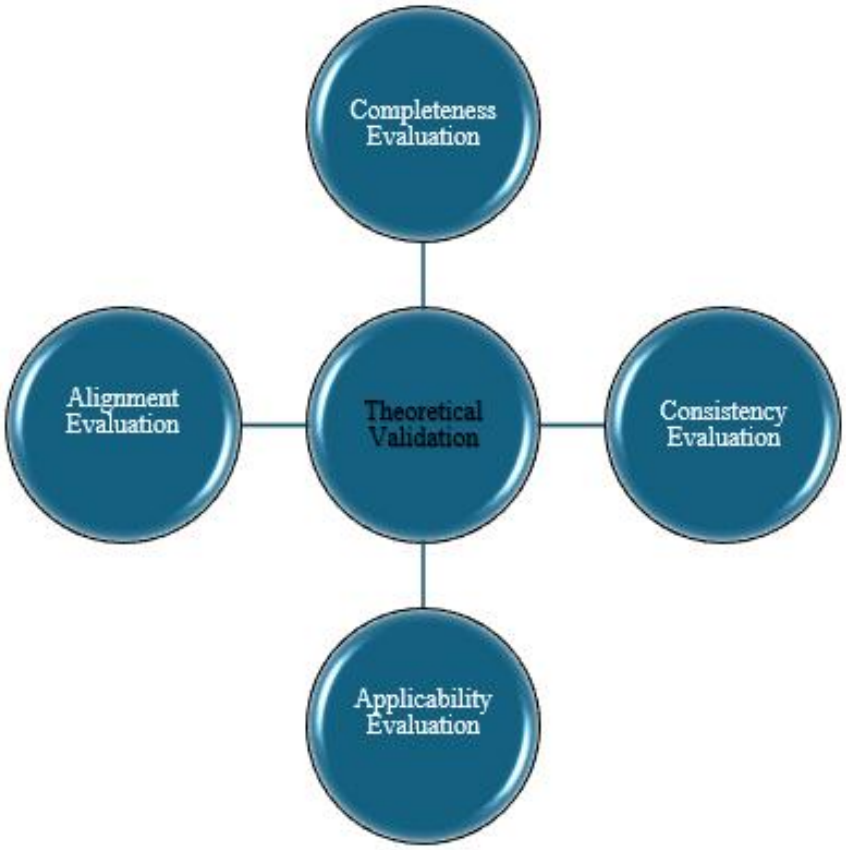
Continuous Improvement: Assesses organizational learning, corrective actions, governance optimization, and process enhancement.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

## Theoretical Validation of the Framework

The proposed framework underwent a theoretical validation (as shown in Figure 8) to ensure logical soundness, conceptual consistency, and alignment with Design Science Research principles. Instead of relying on empirical data, this validation process evaluated whether the framework effectively incorporates key COBIT 2019 and ISO/IEC 27001 concepts and requirements. This method helps validate the framework's comprehensiveness, relevance, and suitability for supporting information security governance maturity assessments in higher education.

**Figure 8.** The validation results indicate that the framework meets essential design and evaluation criteria.




The framework demonstrates its completeness by assimilating strategic governance objectives, operational security controls, performance management mechanisms, and improvement processes. Consistency is evident as the integrated components are conceptually aligned, linking governance goals with security management requirements. Its applicability lies in addressing common governance challenges in higher education, such as decentralized structures and diverse stakeholder environments. Aligned with international standards and governance frameworks, the framework confirms its strong alignment.

## Comparative Analysis of Existing Frameworks

A comparative analysis (Figure 9) was undertaken to evaluate how the proposed framework measures up against existing information security governance and maturity assessment methods. The analysis compared COBIT 2019, ISO/IEC 27001, and other established frameworks to identify similarities and differences. The findings indicate that integrating COBIT 2019 and ISO/IEC 27001 delivers a more balanced approach by merging governance objectives with practical security management needs, thus making the proposed framework especially apt for higher education institutions.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

**Figure 9.** The comparative analysis shows that the integrated framework addresses shortcomings present in individual frameworks and maturity assessment methods.

| Compared to COBIT 2019: | Compared to ISO/IEC 27001: | Compared to Existing Maturity Models: |
|---|---|---|
| The proposed framework extends governance assessment by incorporating operational information security management requirements. | The framework expands operational security management by integrating governance oversight and strategic performance measurement. | The framework provides a more comprehensive assessment structure specifically tailored to higher education institutions. |

**Contributions of the Proposed Framework**

The new framework offers significant academic and practical contributions to the field of information security governance. Theoretically, it merges governance and information security management principles, extends maturity assessment literature, and demonstrates the application of Design Science Research in cybersecurity governance framework development. Practically, it outlines a structured approach for governance maturity assessment, supports governance improvement planning, strengthens alignment between governance and security management, and aids higher education institutions in informed cybersecurity decision-making. These contributions enhance the framework's value and applicability for researchers and practitioners alike.

Theoretical Contributions:

- Integration of governance and information security management theories.
- Extension of maturity assessment literature.
- Application of Design Science Research in cybersecurity governance.

Practical Contributions:

- Structured governance maturity assessment.
- Governance improvement planning.
- Better alignment between governance and security management.
- Support for cybersecurity decision-making within higher education institutions.

These contributions underscore the importance and utility of the proposed framework.

## DISCUSSION

The study's results demonstrate that governance and information security management frameworks possess complementary attributes that can be effectively integrated. COBIT 2019 establishes governance structures and accountability frameworks, while ISO/IEC 27001 specifies operational requirements and security mechanisms. This merge addresses a significant gap identified in the literature, which is the separation of governance evaluation from operational security management.

The proposed framework provides a cohesive approach to evaluate both strategic and operational components of information security governance. This is particularly pertinent to higher education institutions as it addresses the intricate nature of academic governance while supporting assessments of cybersecurity maturity and ongoing advancement. The synthesis of findings, conclusions, recommendations, contributions to knowledge, practical implications, limitations, and directions for future research highlight the significance of the proposed Integrated Information Security Governance Maturity Assessment Framework for Higher Education Institutions.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

This study aimed to bridge the gap arising from the absence of a comprehensive maturity assessment model integrating principles of information security governance with the demands of operational security management. By consolidating COBIT 2019 and ISO/IEC 27001, this research developed a theoretically informed framework to support governance maturity assessment and continuous improvement within higher education contexts.

**Summary of the Study**

The increasing reliance of higher education institutions on digital technologies has amplified the need for effective information security governance. Universities manage vast amounts of sensitive data and confront increasingly complex cybersecurity threats. Consequently, governance mechanisms aligning security goals with institutional objectives have become vital.

Literature Reviews suggest that COBIT 2019 and ISO/IEC 27001 are among the most acknowledged frameworks for governance and information security management. However, numerous studies explore these frameworks in isolation, leading to disjointed governance assessment methods. To address this constraint, the study employed a Design Science Research approach to create an Integrated Information Security Governance Maturity Assessment Framework.

This framework emerged through systematic analysis of governance goals, information security needs, maturity model concepts, and specific requirements of higher education governance. The final framework integrates strategic governance oversight with operational security management needs, offering a structured approach for maturity assessment and ongoing improvement.

**Summary of Findings**

The study highlighted several key findings. Firstly, the analysis verified that COBIT 2019 and ISO/IEC 27001 possess complementary aspects. COBIT 2019 offers governance structures, accountability frameworks, and performance management processes, while ISO/IEC 27001 specifies operational requirements for managing information security.

Secondly, cross-framework mapping demonstrated strong alignment between governance objectives and information security management needs. Numerous governance domains share common goals related to leadership, risk management, monitoring, compliance, and continuous improvement.

Thirdly, the integration process identified five primary governance dimensions collectively representing information security governance maturity in higher education institutions:

- Governance and Leadership
- Risk and Compliance Management
- Security Operations and Control Management
- Monitoring and Performance Evaluation
- Continuous Improvement and Governance Optimization

Fourth, the study devised a five-level maturity model to support structured evaluations of governance capability and organizational readiness. Theoretical validation confirmed the framework satisfies the criteria of completeness, consistency, applicability, and alignment with internationally recognized standards.

## CONCLUSIONS

This study sought to develop an Integrated Information Security Governance Maturity Assessment Framework for Higher Education Institutions by combining the governance principles of COBIT 2019 with the information security management requirements of ISO/IEC 27001.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

The findings suggest that information security governance necessitates a balanced approach blending governance oversight with operational security management. Although COBIT 2019 and ISO/IEC 27001 are individually valuable, neither provides a comprehensive maturity assessment model specifically suited for higher education.

By uniting the strengths of both frameworks, the proposed model offers a more complete method for assessing governance capability, security management practices, and continuous improvement efforts.

The study also illustrated that Design Science Research is an effective methodology for developing governance assessment frameworks. Through a systematic process of problem identification, framework design, and theoretical evaluation, the study produced a framework that is both academically rigorous and beneficial.

The resulting framework provides a structured means of evaluating information security governance maturity and identifying areas for further development within higher education institutions.

This study contributes to knowledge in multiple ways. First, it enhances the literature on information security governance by merging governance theory, information security management principles, and maturity assessment concepts into a unified framework.

Secondly, it contributes methodologically by demonstrating how Design Science Research can be applied to creating governance maturity assessment frameworks.

Thirdly, it offers practical value by providing university administrators, IT managers, governance officers, and policymakers with a tool that supports governance assessment, cybersecurity planning, benchmarking, compliance, and strategic decision-making.

The findings also have significant implications for higher education institutions. As universities operate in increasingly complex digital landscapes, they encounter growing cybersecurity risks, diverse stakeholder expectations, and evolving regulatory demands. These challenges necessitate governance approaches that promote accountability, risk management, and continuous improvement. The proposed framework offers institutions a practical way to evaluate governance maturity, identify weaknesses, and prioritize improvement measures.

By incorporating governance and information security management viewpoints, higher education institutions can enhance cybersecurity resilience, bolster governance effectiveness, and advance their long-term digital transformation goals.

Overall, the study fulfilled its primary objective of developing an Integrated Information Security Governance Maturity Assessment Framework coupling governance objectives and information security management requirements into a comprehensive maturity assessment model. The framework establishes a foundation for future empirical validation and implementation studies and provides a practical contribution to enhancing information security governance in higher education institutions.

**Recommendations**

Based on the study's findings and conclusions, the following recommendations are suggested.

For Higher Education Institutions

1. Adopt integrated governance strategies uniting governance oversight and operational security management.
2. Conduct periodic information security governance maturity assessments using structured maturity models.
3. Enhance governance leadership involvement in cybersecurity planning and oversight activities.
4. Align institutional cybersecurity initiatives with governance objectives and risk management strategies.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

5. Establish continuous improvement mechanisms to support governance optimization.

For Policymakers and Regulatory Bodies

1. Encourage the adoption of internationally recognized governance and security standards.
2. Develop sector-specific governance guidelines for higher education institutions.
3. Promote cybersecurity governance awareness and capability development.

For Researchers

1. Apply the framework within actual institutional environments.
2. Conduct comparative studies across multiple universities.
3. Expand framework validation through expert evaluation and empirical testing.
4. Investigate the relationship between governance maturity and cybersecurity performance outcomes.

**Limitations of the Study**

Several limitations need to be acknowledged.

1. The study centered on conceptual framework development and did not include empirical implementation or field testing.
2. The framework was created through literature synthesis and theoretical analysis instead of organizational data collection.
3. The study concentrated explicitly on higher education institutions and may require adaptation for use in other sectors.

Despite these limitations, the framework offers a solid theoretical foundation for future empirical research and practical application.

Future Research Directions

The researchers will conduct a pilot implementation of the study in selected universities and colleges to empirically validate the effectiveness and practicality of the proposed framework. As part of this process, they will develop and provide comprehensive guidelines for integrating COBIT 2019 and ISO/IEC 27001, including detailed mapping procedures and assessment criteria. Furthermore, comparative case studies across various types of higher education institutions will be carried out to evaluate the framework's adaptability and applicability in diverse educational environments.

Future studies might extend this research in numerous ways.

1. Researchers could undertake empirical validation studies involving universities and colleges.
2. Future investigations might develop assessment instruments and maturity scoring mechanisms based on the proposed framework.
3. Comparative international studies might explore differences in governance maturity across institutions and regions.
4. Researchers might integrate additional frameworks such as NIST Cybersecurity Framework, ITIL, or ISO 31000 into the maturity assessment model.
5. Longitudinal studies might examine governance maturity progression over time and analyze the impact of governance improvement initiatives on cybersecurity outcomes.

## REFERENCES

1. AlGhamdi, S., & Win, K. T. (2020). Information security governance challenges and critical success factors: A systematic review. Computers & Security, 99, 102030.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026


2. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions. Applied Sciences, 10(10), 366.
3. Alkhaldi, F. M., Hammami, S. M., & Uddin, M. A. (2017). Understanding value characteristics toward a robust IT governance application in private organizations using the COBIT framework. International Journal of Engineering Business Management, 9, 1–12. https://doi.org/10.1177/1847979017703779.
4. Alsalem, H., Yahya, Y., & Elias, N. F. (2026). Authentic digital interaction with e-government: A systematic review of key determinants. Information (Switzerland), 17(5). https://doi.org/10.339/info17050427.
5. Bianchi, I. S., Sousa, R. D., & Pereira, R. (2021). Information technology governance for higher education institutions: A multi-country study. In Informatics, Multidisciplinary Digital Publishing Institute, 8(2), 26.
6. Budimir, S., Fontaine, J. R., Huijts, N. M., Haans, A., Loukas, G., & Roesch, E. B. (2021). Emotional reactions to cybersecurity breach situations: A scenario-based survey study. J Med Internet Res, 23(8), e24879. https://doi.org/10.2196/24879.
7. Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. Information, 13(4), 192.
8. Cole-Walker, E. (2026). Reevaluating the mission of higher education: Meeting our cybersecurity challenges together. Educause Review.
9. Culot, G., Nassimbeni, G., Orzes, G., & Sartor, M. (2023). The ISO/IEC 27001 information security management standard: Literature review.
10. De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). COBIT as a framework for enterprise governance of IT. In Management for Professionals: Part F574 (pp. 125–162). Springer Nature. https://doi.org/10.1007/978-3-030-25918-1_5.
11. Fouad, N. S. (2021). Securing higher education against cyberthreats. Journal of Cyber Policy, 6(2), 137–154.
12. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.
13. ISACA. (2019). COBIT 2019 framework: Governance and management objectives. ISACA.
14. ISO/IEC 27001:2022. Information security, cybersecurity, and privacy protection — Information security management systems — Requirements. International Organization for Standardization. (2022). ISO/IEC 27001:2022 information security, cybersecurity, and privacy protection — Information security management systems — Requirements.
15. Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. J Bus Ethics, 137(3), 551–69. https://doi.org/10.1007/s10551-015-2565-9.
16. Merchan-Lima, J., Astudillo, D., Tello Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2020). Information security management frameworks and strategies in higher education institutions: A systematic review. Annals of Telecommunications, 76. 10.1007/s12243-020-00783-2.
17. Mora, M., Gómez, J. M., Wang, F., & Díaz, E. O. (2021). A review of the IT service design process in agile ITSM frameworks. In Balancing Agile and Disciplined Engineering and Management Approaches for IT Services and Software Products (pp. 45–68). IGI Global.
18. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77.
19. Sears, C. R., & Cunningham, D. R. (2024). Individual differences in psychological stress associated with data breach experiences. J Cybersecur. Priv, 4(3), 594–614. https://doi.org/10.339/jcp4030031.
20. Sengik, A. R., Lunardi, G. L., Bianchi, I. S., & Wiedenhöft, G. C. (2022). Using design science research to propose an IT governance model for higher education institutions. Education and Information Technologies, 27(8), 11285–11305. https://doi.org/10.1007/s10639-022-11088-3.
21. Shipman, A., & Watkins, S. (2020). ISO/IEC 27701:2019: An introduction to privacy information management. IT Governance Publishing.
22. Shivashankarappa, S., Rajendran, J., & Bhaskaran, V. (2012). Adoption of ITIL framework in higher education institutions: Challenges and benefits. International Journal of Information Systems in the Service Sector, 4(3), 35–52.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

23. Tocto-Cano, E., et al. (2020). Maturity models in universities: A systematic review. Information, 11(10), 466.
24. Ulven, J. B., & Wangen, G. (2021). Cybersecurity risks in higher education. Future Internet, 13(2), 39.
25. Vaishnavi, V., & Kuechler, W. (2015). Design science research methods and patterns. CRC Press.
26. Winniford, M., Conger, S., & Erickson-Harris, L. (2009). Confusion in the ranks: IT service management practice and terminology. Information Systems Management, 26(2), 153–163.
27. Zúñiga, D. R., Lira, P. L., Navarro, A. C., Peña, M. D., Caselli Benavente, N., Moraga, D. L., Rogget, M. R., & González, J. P. M. (2025). Agile audit proposal for ISO IEC 27001 standard implementation in higher education faculties. Communications in Computer and Information Science, 2347 CCIS, 421–437. https://doi.org/10.1007/978-3-031-84078-4_29.