

Integrating ICT Governance and Information Security Management in Higher Education: A Context-Sensitive Conceptual Framework

Nor Azah binti Jusoh¹, Juhary bin Ali¹

¹ City Graduate School, City University Malaysia, Malaysia

ABSTRACT: Digital dependence has made ICT governance and information security management central to the continuity and quality of higher education. Universities must guide technology investment, protect information assets and sustain critical services, yet these responsibilities are often addressed through separate structures, policies and operational practices. This conceptual paper develops a context-sensitive framework for integrating ICT governance with an Information Security Management System (ISMS) in higher education institutions. The framework is derived through an integrative conceptual synthesis of higher education literature, Socio-Technical Systems Theory, the Resource-Based View, ISO/IEC 38500:2024, COBIT 2019 and ISO/IEC 27001:2022. It comprises five interrelated layers: ICT Governance, ISMS, Operational Information Security Practices, Organisational Efficiency Support and Digital Resilience Support. Seven cross-cutting enablers connect the layers: leadership commitment, competency development, security awareness and culture, communication and coordination, policy documentation and compliance, resource and capability management, and continual improvement. Socio-technical alignment and a continual feedback loop provide the framework's integrating logic. The framework is intended as a guide for contextual analysis and organisational improvement. It is not a causal model, maturity model, audit instrument or claim of certification readiness. Empirical evaluation is required before its practical effects can be established.

KEYWORDS - digital resilience, higher education, ICT governance, information security management system, integrated framework, organisational efficiency

I. INTRODUCTION

Universities rely on digital platforms, cloud services, institutional data, learning systems, research infrastructure and online administration. These resources support core academic and management functions, but they also create dependencies that can affect the whole institution when services are disrupted or information is compromised. Higher education institutions therefore need arrangements that connect technology direction, information protection and service continuity rather than treating them as unrelated technical matters [1], [2], [3].

ICT governance provides direction, accountability and oversight for the current and future use of technology. An Information Security Management System (ISMS) provides a structured approach to defining scope, managing information security risks, operating controls, evaluating performance and supporting continual improvement. The two domains are closely related, but they are not interchangeable. Governance determines institutional direction and decision authority, while an ISMS organises the management of information security risk. Operational practices translate both into day-to-day action and evidence.

Integration remains difficult in higher education because decision-making may be distributed across central units, faculties and specialised centres. Universities also serve diverse users, maintain legacy systems, operate

under public accountability and face continuing pressure to introduce new digital services. In such settings, separate governance and security arrangements may lead to duplicated effort, unclear ownership, inconsistent priorities or gaps between policy and practice.

This paper addresses that problem by proposing a context-sensitive conceptual framework for higher education. It asks how ICT governance, ISMS requirements, operational security, organisational efficiency and digital resilience can be connected without collapsing their different purposes. The contribution is a transparent architecture of five layers, seven cross-cutting enablers, socio-technical alignment and continual feedback. The framework is deliberately non-causal. It identifies relationships that require organisational attention but does not claim that their presence automatically produces efficiency, resilience or compliance.

II. LITERATURE REVIEW

2.1 ICT Governance in Higher Education

ICT governance concerns the system by which the use of technology is directed and controlled. It includes decision rights, accountability, strategic alignment, resource stewardship, risk oversight, performance review and relationships among governing bodies, management and operational functions. Effective governance requires more than a committee or policy. Decisions must be translated into priorities, assigned responsibilities, resource choices, monitoring and corrective action.

Higher education introduces distinctive governance conditions. Institutional missions combine teaching, research, community engagement and administration, while technology authority may be dispersed. Bianchi, Sousa and Pereira argue that higher education needs governance practices suited to its sector rather than the direct transplantation of generic arrangements [1]. Formal structures are therefore only one part of governance. Processes guide planning and review, while relational mechanisms support communication, shared understanding and coordination.

2.2 Information Security Management Systems

ISO/IEC 27001:2022 defines requirements for establishing, implementing, maintaining and continually improving an ISMS [4]. Its management-system orientation distinguishes an ISMS from a collection of security technologies. Firewalls, access controls, monitoring and backups may be necessary, but they do not by themselves establish scope, risk ownership, competence, documented information, management review or continual improvement.

The higher education literature likewise emphasises that information security depends on institutional conditions. Merchan-Lima and colleagues identify frameworks and strategies relevant to university information security while recognising the importance of resources, competencies and organisational participation [2]. Ulven and Wangen show that higher education faces recurring cybersecurity risks across mission-critical assets and varied threat events [3]. These findings point to the need for management discipline, operational evidence and organisational learning.

2.3 Organisational Efficiency and Digital Resilience

Organisational efficiency in a digital unit concerns the coordinated use of people, information, processes and technology to deliver services consistently with proportionate use of resources. Clear responsibilities, standard procedures, automation, reliable information and reduced duplication may support efficiency. Efficiency should not be reduced to cost saving. A process can be inexpensive but inefficient when responsibilities are unclear, incidents recur or corrective work repeatedly consumes staff time.

Digital resilience is the organisational capacity to anticipate, prepare for, withstand, respond to, recover from and learn from disruption affecting digital services. It extends beyond disaster recovery. Backup and restoration provide technical capability, while continuity planning, incident authority, communication, redundancy, testing and post-incident learning provide organisational capability. Efficiency and resilience may create short-term tensions because documentation, redundancy and testing require resources. The proposed framework therefore treats them as support domains that must be considered together, not as guaranteed outcomes.

III. THEORETICAL AND STANDARDS FOUNDATIONS

3.1 Socio-Technical Systems Theory

Socio-Technical Systems Theory (STST) proposes that organisational performance depends on the joint consideration of social and technical subsystems [5], [6]. The social subsystem includes people, roles, authority,

knowledge, relationships and culture. The technical subsystem includes infrastructure, tools, procedures and work processes. A technically sound control may still fail when responsibility is unclear, users do not understand it or operational demands make compliance impractical. STST therefore provides a suitable basis for connecting governance, security management and operational practice.

3.2 Resource-Based View

The Resource-Based View (RBV) explains how organisational resources and capabilities can support sustained performance when they are valuable and effectively organised [7], [8]. In a public university, the relevant value is not limited to competitive advantage. Expertise, institutional knowledge, dependable routines, leadership attention and recovery experience can support reliable services, accountability and adaptation. RBV draws attention to the capabilities required to sustain governance and security after policies have been approved.

3.3 Complementary Standards

ISO/IEC 38500:2024, COBIT 2019 and ISO/IEC 27001:2022 contribute different but complementary forms of guidance. ISO/IEC 38500 focuses on governing responsibility for the effective, efficient and acceptable use of IT [9]. COBIT distinguishes governance from management and links objectives with components such as processes, organisational structures, information and people [10]. ISO/IEC 27001 provides requirements for managing information security risk through a defined and continually improved management system [4]. None should be treated as a substitute for the others.

Table 1. Complementary Foundations

Source	Primary contribution	Role in the framework
ISO/IEC 38500:2024	Governing responsibility for the use of IT	Direction, accountability and oversight
COBIT 2019	Governance and management objectives and components	Connections among structures, processes, information and people
ISO/IEC 27001:2022	Risk-based information security management requirements	Scope, risk treatment, competence, evaluation and improvement
STST	Joint consideration of social and technical systems	Cross-layer alignment
RBV	Development and organisation of resources and capabilities	Competency, knowledge, routines and recovery capability

IV. CONCEPTUAL DEVELOPMENT APPROACH

This is a conceptual paper rather than a systematic review or empirical case study. Its purpose is theory and framework development through an integrative synthesis of established literature, theory and international standards directly relevant to ICT governance and information security management in higher education. The source base combines peer-reviewed higher education studies, foundational theoretical work and authoritative standards. No claim is made that the literature set is exhaustive.

Framework development followed four analytical stages. First, the literature was examined to identify the distinct purposes of ICT governance, ISMS, operational security, organisational efficiency and digital resilience. Second, ISO/IEC 38500, COBIT and ISO/IEC 27001 were compared to identify complementary responsibilities and management requirements. Third, STST and RBV were used to explain relational and capability conditions. Fourth, the resulting concepts were organised into layers and cross-cutting enablers, with a traceability check to ensure that each component had a clear conceptual basis.

The five layers were formed by grouping the selected concepts according to their primary organisational function. The seven enablers were retained where the literature, theory and standards indicated a recurring condition that operates across more than one layer. This procedure provides conceptual traceability; it does not represent frequency counting or empirical validation.

The approach preserves important boundaries. Standards inform the framework but are not merged into a new standard. Theory explains relationships but does not demonstrate compliance or causality. The framework is a reasoned conceptual proposition that requires empirical evaluation before claims can be made about its usability, effects or transferability.

V. PROPOSED CONCEPTUAL FRAMEWORK

5.1 Framework Architecture

The proposed framework contains five interrelated layers, seven cross-cutting enablers, socio-technical alignment and a continual feedback loop. The layers represent organisational domains rather than a fixed implementation sequence. Institutions may strengthen several layers at the same time according to risk, capacity and strategic priority. This arrangement retains the distinct purposes of governance, management-system discipline and operational control while making their relationships explicit.

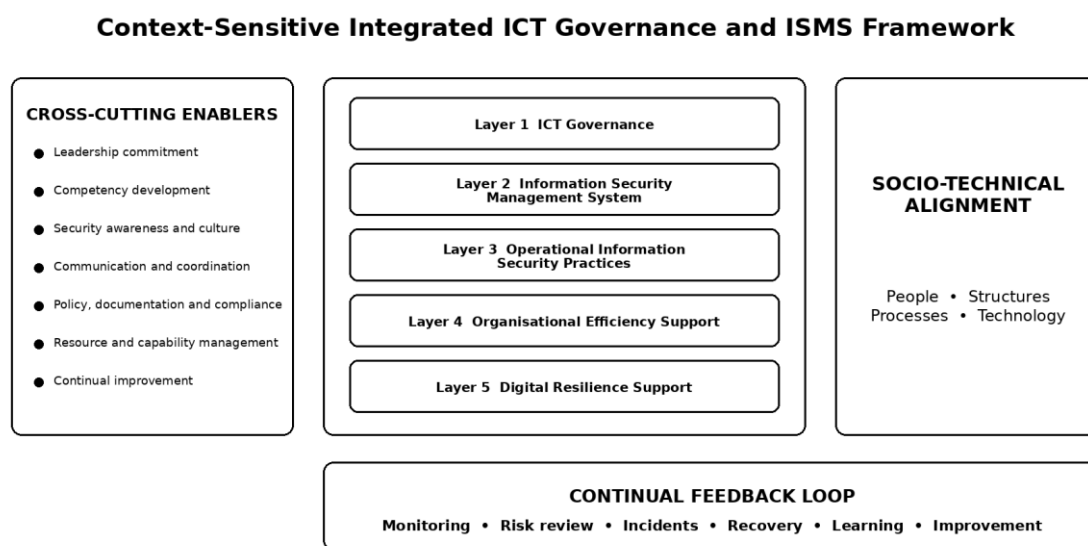


Fig. 1. Proposed context-sensitive integrated framework

5.2 Five Interrelated Layers

Layer 1, ICT Governance, provides institutional direction and oversight. It covers governance structures, strategic alignment, accountability, policy, resource governance, risk oversight, performance monitoring and review. Its role is to clarify why technology and security priorities matter, who holds decision authority and how evidence informs governing decisions.

Layer 2, Information Security Management System, organises information security through a defined scope and risk-based management cycle. It includes organisational context, leadership, policy, risk assessment and treatment, responsibilities, competence, documented information, operational planning, performance evaluation, management review and improvement.

Layer 3, Operational Information Security Practices, translates authorised direction and risk treatment into daily activity and evidence. It includes access management, asset protection, monitoring, incident management, security in change, backup, recovery, continuity activity, compliance and operational records. It is the main bridge between formal policy and observable practice.

Layer 4, Organisational Efficiency Support, keeps coordination, consistency, appropriate resource use, decision support, service delivery, reduced duplication and learning visible in governance and security decisions. It is a support domain because the framework may create enabling conditions but cannot guarantee efficiency outcomes.

Layer 5, Digital Resilience Support, covers anticipation, preparedness, resistance, response, recovery, critical-service continuity, adaptation and learning. It connects technical recovery capability with authority,

communication, competence and organisational review. Resilience is treated as an evolving capability rather than a one-time project.

Table 2. Layers and Principal Purposes

Layer	Principal purpose
1. ICT Governance	Set direction, accountability, oversight and resource priorities
2. ISMS	Organise information security through a scoped, risk-based management cycle
3. Operational Practices	Apply controls and produce operational evidence
4. Efficiency Support	Keep coordination, consistency, resource use and service delivery visible
5. Resilience Support	Connect preparedness, response, recovery, continuity and learning

5.3 Seven Cross-Cutting Enablers

Leadership commitment provides authority, prioritisation and sustained attention. Competency development builds the knowledge and practical skills needed to govern risk, manage security, operate services and recover from disruption. Security awareness and culture connect formal policy with daily behaviour and shared responsibility.

Communication and coordination link governing bodies, management, technical teams, service owners and users. Policy, documentation and compliance provide clarity, traceability, organisational memory and evidence. Resource and capability management aligns people, time, finance, knowledge and technology with priority risks. Continual improvement converts monitoring results, incidents, exercises and environmental change into learning and corrective action.

These enablers cross all five layers because their influence is not confined to a single domain. Competency is required in governance, risk management, operations and recovery. Documentation supports both routine consistency and crisis coordination. Leadership affects priority, resources and follow-through. Placing the enablers across the framework avoids reproducing the fragmentation the framework is intended to address.

Table 3. Cross-Cutting Enablers

Enabler	Organisational function
Leadership commitment	Authority, priority and sustained attention
Competency development	Role-specific knowledge and practical capability
Security awareness and culture	Shared understanding and responsible behaviour
Communication and coordination	Connections across governance, management and operations
Policy, documentation and compliance	Clarity, traceability, memory and evidence
Resource and capability management	Alignment of people, time, finance, knowledge and technology
Continual improvement	Learning and corrective action from monitoring, incidents and change

5.4 Socio-Technical Alignment and Continual Feedback

Socio-technical alignment requires decisions to consider people, structures, processes and technology together. The continual feedback loop connects performance monitoring, risk review, incidents, service experience, recovery exercises and external change with governance review and improvement. Useful feedback identifies

what happened, what evidence is available, which assumptions changed, who owns the response and what adjustment is proportionate. This prevents the framework from becoming static.

VI. DISCUSSION

The framework makes the integration mechanism explicit. ICT governance supplies direction and authority; the ISMS provides risk-based management discipline; and operational practices implement authorised controls and produce evidence. Efficiency and resilience remain visible as organisational concerns. The cross-cutting enablers connect these domains, while feedback supports review and adaptation.

This architecture avoids two common reductions. The first is technology-only security, in which controls are implemented without sufficient attention to roles, culture, coordination or learning. The second is documentation-only management, in which policies exist without dependable operational enactment. Both are socio-technically incomplete. STST explains the reciprocal relationships across social and technical elements, while RBV explains why knowledge, routines, leadership attention and recovery capability require deliberate development and organisation.

The framework also clarifies the relationship among standards. ISO/IEC 38500 informs governing responsibility, COBIT assists in articulating governance and management components, and ISO/IEC 27001 informs disciplined management of information security risk. Context-sensitive use requires institutions to examine their mandates, decision structures, service criticality, resources, technology environments, risks and cultures. Direct replication without contextual analysis would be inconsistent with the framework's purpose.

VII. PRACTICAL AND THEORETICAL IMPLICATIONS

University leaders can use the framework to examine whether security and continuity priorities are visible in governance forums, whether responsibilities are assigned and whether monitoring evidence informs resource and risk decisions. ICT and security managers can map existing arrangements across the layers and identify missing connections. Operational teams can use the framework to link evidence from access reviews, incidents, changes, backups, restoration and exercises to organisational learning.

The theoretical contribution lies in combining STST and RBV within a non-causal integration architecture. STST provides the relational logic across social and technical domains, while RBV explains the capability base that allows those relationships to operate over time. The framework therefore connects organisational alignment with capability development without converting either theory into predefined variables or causal hypotheses.

VIII. LIMITATIONS AND FUTURE RESEARCH

The framework is based on conceptual synthesis and has not been implemented, tested or externally validated. The selected literature is relevant but not exhaustive, and the framework does not establish maturity levels, scoring rules, audit criteria or certification readiness. Its practical relevance and transferability cannot be assumed.

Future research should begin with structured stakeholder review to assess clarity, relevance, missing relationships, feasibility and unintended consequences. Participatory case studies could then adapt the framework to institutional settings, while longitudinal research could examine changes in responsibilities, practices and evidence during implementation. Comparative studies may assess contextual variation across universities. Quantitative testing should follow only after constructs and relationships have been clearly operationalised.

IX. CONCLUSION

This paper proposes a context-sensitive framework for integrating ICT governance and information security management in higher education. Five interrelated layers connect governance direction, ISMS discipline, operational information security, organisational efficiency support and digital resilience support. Seven cross-cutting enablers, socio-technical alignment and continual feedback provide the conditions through which these domains can be considered together.

The framework's value lies in integration without overstatement. It preserves the different purposes of governance, management systems and operational control while showing where relationships and capabilities require attention. It is a conceptual guide for analysis and improvement, not a validated causal model, maturity model, audit instrument or evidence of certification readiness. Its contribution should be tested and refined through transparent empirical research.

DECLARATIONS

10.1 Ethics Approval and Consent to Participate

Not applicable. This conceptual paper did not involve human participants or the collection of personal data.

10.2 Data Availability

No primary dataset was generated or analysed for this conceptual paper.

10.3 Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

10.4 Conflict of Interest

The authors declare no conflict of interest.

10.5 Acknowledgements

The authors acknowledge the scholarly and standards-based sources that informed the conceptual development of the framework.

REFERENCES

- [1] I. Scalabrin Bianchi, R. Dinis Sousa, and R. Pereira, Information technology governance for higher education institutions: A multi-country study, *Informatics*, 8(2), 2021, 26. <https://doi.org/10.3390/informatics8020026>
- [2] J. Merchan-Lima, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, G. Lopez-Fonseca, and D. Quiroz, Information security management frameworks and strategies in higher education institutions: A systematic review, *Annals of Telecommunications*, 76(3-4), 2021, 255-270. <https://doi.org/10.1007/s12243-020-00783-2>
- [3] J. B. Ulven and G. Wangen, A systematic review of cybersecurity risks in higher education, *Future Internet*, 13(2), 2021, 39. <https://doi.org/10.3390/fi13020039>
- [4] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements (Geneva: ISO, 2022).
- [5] G. Baxter and I. Sommerville, Socio-technical systems: From design methods to systems engineering, *Interacting with Computers*, 23(1), 2011, 4-17. <https://doi.org/10.1016/j.intcom.2010.07.003>
- [6] P. M. Bednar and C. Welch, Socio-technical perspectives on smart working: Creating meaningful and sustainable systems, *Information Systems Frontiers*, 22(2), 2020, 281-298. <https://doi.org/10.1007/s10796-019-09921-1>
- [7] J. Barney, Firm resources and sustained competitive advantage, *Journal of Management*, 17(1), 1991, 99-120. <https://doi.org/10.1177/014920639101700108>
- [8] M. Wade and J. Hulland, The resource-based view and information systems research: Review, extension, and suggestions for future research, *MIS Quarterly*, 28(1), 2004, 107-142. <https://doi.org/10.2307/25148626>
- [9] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 38500:2024 Information technology - Governance of IT for the organization (Geneva: ISO, 2024).
- [10] ISACA, COBIT 2019 framework: Introduction and methodology (Schaumburg, IL: ISACA, 2018).