Journal of Governance Risk Management Compliance and Sustainability (JGRCS), Vol. 6 No. 1 (2026) https://doi.org/10.31098/jgrcs.v6i1.4119

Research Paper

Strengthening Academic Libraries: Quality Assurance Planning and Development Office's Role in Digital Resilience and Risk Management

Mary Rose Montano*, Ronald A. Gonzales, Simplicio P. Alba, Anna Rhea C. Opeña, Marilyn R. Garma, Armando A. Salenga Jr., Francis Eduard T. Malitig, Lyka B. Rodelas, Michael S. Navarro
City College of Calamba, Philippines

Received: January 8, 2026	Revised : March 25, 2026	Accepted : April 25, 2026	Online : April 30, 2026

Abstract

Libraries increasingly face complex risks threatening both physical and digital collections; however, empirical qualitative evidence on how institutional risk governance structures operationalize digital resilience remains limited. This qualitative case study examines the risk preparedness of 20 academic libraries within a bounded higher education governance context through open-ended questionnaires and policy document review. Findings indicate that while basic physical safeguards and manual digital backups are widely practiced, libraries lack formalized disaster recovery frameworks, cybersecurity protocols, and governance-aligned digital risk strategies. Crucially, the Quality Assurance, Planning, and Development Office (QAPDO) emerges not merely as a support unit but as a governance leverage point, capable of translating risk awareness into institutional obligation through policy alignment, strategic planning, accreditation-linked monitoring, capacity building, and resource mobilization. The study advances institutional resilience scholarship by reframing digital resilience from a technical or library-specific concern into an institutional governance capacity, demonstrating how QAPDO can re-couple fragmented library practices with central quality assurance systems. The study proposes a governance-centered conceptual framework that positions QAPDO as the mediating mechanism between institutional risk environments and sustainable digital resilience outcomes, offering a replicable model for embedding resilience into higher education library governance.

Keywords: *Library Resilience, Disaster Risk Management, Digital Resilience, Quality Assurance, QAPDO, Future-Proofing*

INTRODUCTION

Libraries, long regarded as vital repositories of knowledge, memory, and culture, serve as key pillars of educational institutions and community development. With the growing reliance on digital systems, these institutions now manage not only physical collections but also vast arrays of digital resources. However, this dual responsibility exposes libraries to a widening range of disruptions—natural disasters, cyberattacks, system failures, and financial constraints—that threaten both their physical infrastructure and the integrity, availability, and security of their digital assets.

Despite the essential role libraries play in ensuring equitable access to information, many remain ill-equipped to address such threats comprehensively. Literature on library risk management has predominantly focused on physical disaster planning (Dada et al., 2025; Brown, 2021) or on digital preservation in isolation (Garnett, 2019; Lee, 2025). However, a critical gap remains in understanding how institutional governance structures—specifically quality assurance and planning units—function as central mechanisms for integrating and sustaining digital resilience within libraries. While studies acknowledge the importance of strategic planning and institutional support (Cox, 2023; Hoving, 2025), the specific role of offices like the Quality

Corresponding author's email: mfmontano@ccc.edu.ph

Assurance, Planning, and Development Office (QAPDO) in operationalizing risk governance remains underexplored and theoretically underdeveloped.

In this context, QAPDO is not merely an administrative unit but a core governance mechanism responsible for institutional alignment, policy development, resource allocation, and compliance with quality standards (Jesry et al., 2022). Its mandate spans strategic foresight, capacity building, and cross-functional coordination—functions that are essential for embedding risk management into the institutional fabric. Yet, its potential to bridge the gap between high-level quality assurance and on-the-ground digital resilience in libraries has not been empirically examined.

Recognizing this governance gap, this study moves beyond descriptive accounts of library preparedness to investigate how QAPDO functions as an institutional actor in risk governance. Rather than asking only what challenges exist, we examine how governance structures enable or constrain resilience-building. Accordingly, the study is guided by the following research questions:

Central Question:

What is the current level of risk preparedness in libraries, as measured by the presence of formal risk management plans for physical and digital collections, and how can QAPDO enhance their resilience through effective planning and support mechanisms?

Specifically, it seeks to answer the following corollary questions:

1. What formal risk management and disaster recovery plans currently exist in libraries for both physical and digital collections?
2. What are the perceived challenges and limitations faced by libraries in developing and implementing comprehensive risk management strategies, particularly for digital assets?
3. How do library personnel perceive the role of QAPDO in supporting risk preparedness and resilience planning for library operations?
4. What specific strategies, tools, or institutional mechanisms can be adopted—with QAPDO's support—to enhance digital resilience and ensure service continuity in the face of disruptions?

By exploring the interplay between governance mechanisms and operational resilience, this study contributes a governance-centered perspective to the literature on library risk management. It shifts the focus from technical solutions and isolated policy recommendations to an understanding of how quality assurance units can systematically institutionalize digital resilience, ensuring sustainable service continuity in an increasingly volatile and technology-driven environment

LITERATURE REVIEW

This review moves beyond descriptive summaries by organizing prior studies around four interrelated thematic debates that situate library digital resilience within governance and risk management theory. Rather than treating digital resilience, disaster risk management (DRM), future-proofing, and quality assurance as separate concepts, it integrates them into a unified governance-oriented perspective that highlights how institutional mechanisms enable or constrain resilient library systems.

For this study, digital resilience is defined as an institution's capacity to anticipate, absorb, adapt to, and recover from digital disruptions while sustaining core services and accountability. Risk management refers to the structured identification, assessment, mitigation, and monitoring of threats across physical, digital, human, and organizational domains. Quality assurance is conceptualized as a governance function that embeds accountability, learning, and continuous improvement into institutional processes.

Operational Risk Management vs. Risk Governance in Libraries

In the context of rapid digitalization, libraries have evolved into dynamic centers of digital access, lifelong learning, and community engagement. The integration of technologies such as e-books, self-service systems, and digital platforms has expanded access and reshaped librarians' roles toward facilitating digital literacy and critical information use (Silliman University Library System, 2023). Scholars emphasize that adopting innovative, user-centered technologies is essential for sustaining effective library services amid changing user expectations and institutional pressures (George & Wagwu, 2025).

However, as demonstrated by Rahmani (2025), public libraries—particularly in economically constrained contexts such as Iran—face compounded financial, technological, and human resource risks that hinder this transformation. Financial instability, intensified by economic sanctions and limited public funding, restricts investment in digital infrastructure, electronic collections, and staff development, thereby exacerbating technological limitations and skills gaps. These structural constraints, coupled with growing competition from commercial digital platforms and persistent urban–rural disparities, undermine library relevance and equitable access to information.

Collectively, these findings underscore the urgent need to embed digital resilience and strategic risk management into library planning through sustained investment, policy reform, and continuous capacity-building to ensure that libraries remain resilient, future-ready, and socially inclusive institutions in the digital age.

Digital Resilience as Technical Capacity vs. Institutional Capability

Early scholarship often frames digital resilience as a technical capacity, emphasizing digitization, preservation technologies, backup systems, and recovery tools to mitigate disruption (Garnett, 2019; Gbotosho & Opele, 2025). While such measures enhance operational readiness, they assume that technology alone ensures resilience, overlooking the importance of organizational decision-making, coordination, and governance. Evidence from crises suggests that technical infrastructure cannot sustain resilience without institutional mechanisms guiding its effective deployment and adaptation.

Recent studies reconceptualize digital resilience as an institutional capability embedded within governance structures, leadership practices, and learning systems. For instance, South Korea's COVID-19 response demonstrates that resilience depends on staged processes of sensing, shock absorption, adaptation, and transformation, enabled by regulatory preparedness, cross-sector collaboration, and public trust (Park & Choi, 2025). Digital tools function as enablers whose effectiveness relies on policy coherence, staff capacity, and continuous evaluation (Lee, 2025; Trembach, 2024).

Empirical evidence from academic libraries shows that access to digital platforms, while necessary, is insufficient to counter misinformation and disinformation (Hamad, 2023). Information literacy programs institutionalize resilience by equipping users with skills to evaluate and verify information, shifting libraries from reactive technical interventions to proactive capacity-building.

Sustainable digital resilience thus requires integrating technology with institutional capability. Through quality assurance, planning, and governance, resilience becomes a strategic outcome rather than a technological artifact.

Future-Proofing as Innovation vs. Strategic Risk Anticipation

The concept of future-proofing in library literature is often linked to innovation, emerging technologies, and new service models (Nicholas et al., 2023; Ganesamoorthy & Selvakamal, 2024). While these developments enhance relevance and adaptability, they risk underplaying the role of anticipatory risk governance, particularly in contexts of uncertainty, limited resources, and institutional accountability.

Governance scholarship emphasizes that future-proofing extends beyond technological adoption to include structured foresight, compliance awareness, and alignment with institutional missions (Cox, 2020; Cox, 2023). From this perspective, it represents institutional readiness—the ability to anticipate disruption, manage risks proactively, and sustain core functions during change.

Empirical evidence from Opele (2021) illustrates the dual role of emerging technologies in library education: digitization expands collections and access, while virtual platforms, video conferencing, and social media facilitate global collaboration and knowledge exchange. Yet, these innovations also introduce risks, including skills obsolescence, inequitable access, and governance challenges. Without mechanisms for risk anticipation, innovation alone cannot ensure sustainable outcomes.

Accordingly, this study reframes future-proofing as a governance outcome, realized when libraries embed digital resilience into planning, quality assurance, and decision-making. In this framework, technological advancement functions as an enabler, while strategic preparedness, accountability, and adaptive governance constitute the core of sustainable, institution-wide resilience.

Quality Assurance as Compliance vs. Enabler of Resilience

Quality assurance (QA) in higher education is commonly framed as a compliance-oriented function centred on accreditation, documentation, and performance indicators. However, Jesry et al. (2022) demonstrate that QA systems can also operate as mechanisms of risk governance when monitoring, feedback, and capacity-building are embedded within institutional routines. This shift expands QA beyond control and oversight toward a more strategic, resilience-oriented role.

Within the library context, this distinction is particularly significant. When QA units function solely as evaluators, resilience initiatives tend to be fragmented and reactive. Conversely, positioning QA as a strategic enabler allows the alignment of policies, resources, training, and evaluation processes, thereby institutionalising resilience rather than treating it as an ad hoc response to disruption.

Reframing QA in this way underscores its capacity to operate across organisational systems by integrating risk, processes, and people. Quality professionals are equipped to identify interdependencies and anticipate vulnerabilities before they escalate into crises, supporting evidence-based decision-making at both operational and strategic levels (Koutsochera, 2025). This system's perspective is consistent with the risk-based thinking embedded in contemporary quality management standards, which prioritise prevention, adaptability, and continuous improvement over post hoc correction (ISO 9001:2015).

Embedding quality within organisational culture is therefore central to resilience-building. Procedures alone are insufficient; resilience emerges when quality principles promote shared accountability, learning, and adaptability across functions. As illustrated by Koutsochera (2025), practices such as aligning quality objectives with organisational goals and integrating quality requirements early in operational processes transform compliance into an outcome of well-designed systems rather than an end in itself.

Building on this perspective, the study positions the Quality Assurance, Planning, and Development Office (QAPDO) as a latent governance asset capable of translating resilience

principles into operational practice through structured planning, policy development, and performance monitoring.

Synthesized Conceptual Framework Guiding the Study

The conceptual framework in Figure 1 integrates risk governance, quality assurance, and digital resilience to explain how libraries respond to institutional vulnerabilities. It recognizes that libraries face physical, digital, financial, and human risks that can threaten service continuity, information security, and institutional stability. The framework positions the Quality Assurance, Planning, and Development Office (QAPDO) as the central governance enabler, mediating risk through strategic planning, policy development, capacity-building, resource alignment, and continuous monitoring.

Effective implementation of these governance mechanisms enables stronger digital resilience outcomes, including disaster and digital continuity plans, cybersecurity readiness, sustained service operations, adaptive capacity, and institutional learning. The framework emphasizes that resilience is not merely reactive but a deliberate product of embedded governance processes, allowing libraries to shift from vulnerability to preparedness in a digitally dependent environment.

This framework informs the study's qualitative analysis, guiding coding around: (a) types of risks, (b) perceived and actual QAPDO functions, and (c) resulting resilience capacities or gaps. Grounding analysis in governance theory provides a robust explanation for why digital resilience remains uneven despite widespread awareness of risks.

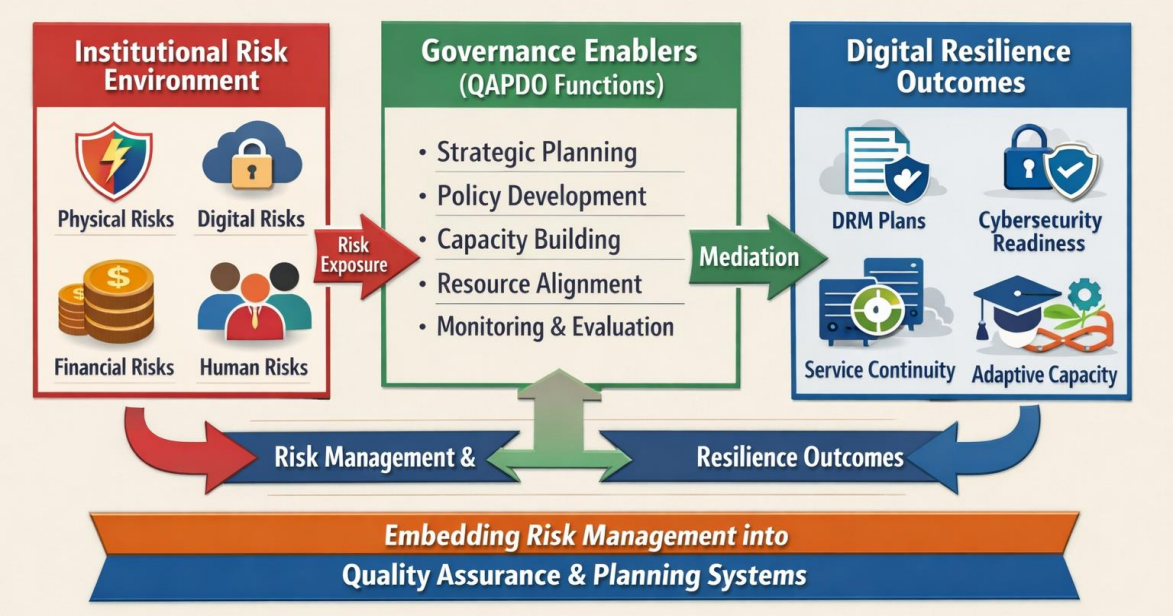

Figure 1. Conceptual Framework

RESEARCH METHOD

Research Design and Case Boundaries

This study employed a qualitative case study design to examine how academic libraries develop risk preparedness and digital resilience and how these efforts are shaped by institutional governance, particularly through the Quality Assurance, Planning, and Development Office (QAPDO). Following Baxter and Jack (2008), the case study approach was selected because it allows in-depth exploration of complex governance processes within real-life institutional contexts.

The case is defined as a bounded, multi-institutional governance context rather than an aggregated sector-wide survey. Specifically, the unit of analysis is academic library risk preparedness and digital resilience practices as embedded within higher education institutions where a formal QAPDO exists. While participants were drawn from multiple higher education institutions, these institutions are treated collectively as one bounded case of governance practice, unified by comparable organizational structures, quality assurance mandates, and regulatory environments. The study does not aim to compare institutions but to identify shared patterns of governance-enabled resilience across a bounded institutional context.

This bounded-case approach enables analytical generalization by illuminating how QAPDO functions as a governance mechanism shaping library risk management, rather than producing statistically representative sectoral claims.

Participants and Unit of Analysis

Using purposive sampling, the study involved 20 library personnel from higher education institutions, including library directors, librarians, IT staff, and frontline personnel with responsibilities related to digital systems and risk management. Participants were selected based on their direct involvement in library operations and their familiarity with institutional planning, disaster preparedness, and digital resource management, ensuring that responses reflected informed, practice-based perspectives.

The unit of analysis was not the individual respondent but institutional practices and shared perceptions of library risk preparedness and digital resilience, as articulated by participants occupying operational and governance-linked roles. This approach enabled the study to move beyond personal experiences toward an examination of how risk management and resilience are understood and enacted at the institutional level, particularly in relation to the perceived role of the Quality Assurance, Planning, and Development Office (QAPDO).

The sample size aligns with established qualitative research standards. A synthesis by Hennink and Kaiser (2021) indicates that thematic saturation is typically achieved within 9–17 interviews in relatively homogenous populations with focused research objectives. Given the participants' shared institutional context and professional backgrounds, the inclusion of 20 respondents was sufficient to capture nuanced patterns, ensure thematic depth, and enhance the credibility and trustworthiness of the findings.

Data Collection Instrument

Data were collected using a structured Google Forms questionnaire composed entirely of open-ended questions, designed to elicit reflective, experience-based responses aligned with the study's governance-oriented research questions. The instrument comprised four sections with a total of 14 open-ended items, covering existing risk management practices, challenges and limitations, perceptions of the Quality Assurance, Planning, and Development Office (QAPDO), and recommended strategies or institutional mechanisms for strengthening digital resilience. Sample prompts asked participants to describe current formal or informal disaster recovery plans for physical and digital collections, identify barriers to comprehensive digital risk management, reflect on QAPDO's role in supporting preparedness and resilience, and propose strategies to enhance digital resilience in library operations. Participants were encouraged to provide detailed narrative responses without word-limit restrictions to allow depth and nuance.

Written responses were intentionally selected over interviews because participants were geographically distributed across institutions, the format allowed respondents to consult institutional documents and policies while answering, and the study's emphasis on governance processes and formal practices favored considered, document-informed accounts rather than

spontaneous verbal responses. This approach is consistent with qualitative research that recognizes written narratives as valid and rigorous data sources for institutional and policy-focused inquiry.

Data Collection Procedure

The Google Forms link was distributed via institutional email. Data collection occurred over four weeks. Responses were automatically compiled and exported into a spreadsheet for organization and analysis. Where responses were brief or ambiguous, follow-up clarification emails were sent to participants, requesting elaboration on specific points.

In addition to participant narratives, institutional documents (e.g., existing risk management plans, disaster protocols, and policy guidelines mentioned by respondents) were reviewed where available to contextualize and triangulate responses.

Data Analysis

Data were analyzed using Braun and Clarke's (2006) six-phase thematic analysis. First, all responses were read repeatedly to achieve familiarization and to identify initial patterns related to risk preparedness, governance roles, and resilience strategies. Next, inductive coding was conducted by segmenting the data into meaningful units focusing on risks, practices, governance functions, challenges, and proposed interventions. These codes were then organized into a working codebook containing definitions and exemplar quotations, which was iteratively refined to minimize overlap and enhance analytic clarity.

Related codes were subsequently clustered into preliminary themes (e.g., Basic Physical Safeguards, Delegated IT Oversight, Governance-Enabled Resilience). These themes were reviewed against the full dataset to ensure internal coherence and clear conceptual boundaries before being further refined, defined, and named. Final themes were interpreted in relation to the study's governance-focused conceptual framework, allowing for theoretically grounded analysis. Coding and theme refinement were conducted by the primary researcher, with peer debriefing undertaken with a qualitative research colleague to review coding decisions, theme development, and interpretive claims, thereby strengthening analytic rigor.

Trustworthiness and Rigor

Several strategies were employed to ensure the trustworthiness of the study. Credibility was enhanced through member checking, wherein summarized interpretations were returned to selected participants to validate the accuracy and meaning of the findings. Dependability was supported by maintaining a clear audit trail that included raw responses, successive coding iterations, the evolving codebook, and analytic memos documenting key methodological and interpretive decisions. To strengthen confirmability, peer debriefing sessions were conducted to challenge assumptions, review theme development, and minimize individual researcher bias. In terms of reflexivity, the researcher acknowledges a professional background in academic quality assurance and planning, which informed sensitivity to governance processes; reflexive memos were maintained throughout the analysis to critically examine how this positionality shaped data interpretation. Collectively, these procedures enhanced methodological transparency and reinforced the analytic rigor of the study.

Ethical Considerations

Ethical considerations were carefully observed throughout the study. Participation was voluntary, and informed consent was obtained from all participants before data collection. To protect confidentiality, institutional names and individual identifiers were anonymized in all

records and reports. All data were stored securely and used solely for academic and research purposes.

FINDINGS AND DISCUSSION

Existing Risk Management and Disaster Recovery Plans for Both Physical and Digital Collections

Analysis of current risk management practices (Table 1) reveals a fragmented, compliance-driven approach, reflecting low institutional capability maturity. Basic measures such as fire protection and manual backups are widespread, yet they operate as isolated technical responses rather than components of an integrated governance system. The reliance on reactive safeguards, coupled with limited digital protocols and formal recovery plans, indicates that libraries function at a survival level, lacking strategic, anticipatory resilience.

This pattern underscores the distinction between technical capacity—tools and infrastructure—and institutional capability, which involves policies, coordination, learning, and accountability. Libraries remain heavily dependent on delegated IT oversight and ad-hoc collaboration instead of embedding risk governance within their organizational structures. Such fragmentation highlights low institutional maturity, where risk management exists as disconnected practices rather than a systematized, monitored, and accountable framework, consistent with Dada et al. (2025) and Edward et al. (2025).

Advancing from fragmented compliance to integrated resilience requires elevating risk management into an institutional capability. This involves not only technical measures and staff training, but also embedding accountability into governance through formal mandates, cross-functional coordination, and alignment with institutional assurance mechanisms such as QAPDO. Without this shift, library preparedness will remain reactive, uneven, and insufficient to address evolving digital and physical threats.

Table 1. Fragmented Risk Preparedness Reflects Low Institutional Capability Maturity

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
PHYSICAL COLLECTIONS					
Basic fire protection (extinguishers, alarms, drills)	"We have fire extinguishers." "Smoke detectors and emergency exits are in place." "Safety drills are conducted regularly."	14	14	Basic Physical Safety Measures	Fire-related emergency tools and procedures are widely adopted, demonstrating minimum safety compliance.
Flood protection and second-floor safety	"Library is on the second floor." "Important items are stored off the floor to prevent water damage."	8	8	Flood and Water Risk Minimization	Location and physical arrangements help mitigate risk from water-related

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
					incidents.
Regular monitoring and inspections	"Collections are regularly inspected." "We conduct pest control and maintenance checks."	5	5	Preventive Maintenance	Proactive inspection and environmental control help prevent avoidable physical threats.
Staff awareness and emergency training	"Staff are trained to respond during emergencies." "Steps and contacts are clearly posted."	7	7	Staff Preparedness	Libraries rely on trained personnel and accessible instructions to minimize disruption.
Manual documentation of priority items	"Essential items are documented and prioritized for recovery."	2	2	Preservation Planning	Some libraries maintain item-level documentation to guide post-disaster recovery.
Response coordination with other departments	"We coordinate with the Property Management Office." "School management supports recovery protocols."	5	5	Interdepartmental Collaboration	Libraries rely on external departments for formal execution and support of recovery operations.
DIGITAL COLLECTIONS					
Basic data backup (USB, Google Drive, hard drives)	"We use USB and Google Drive for backup." "Files are stored in a shared folder."	11	11	Basic Backup Practices	Data protection is ensured through simple, user-driven backup strategies.
Advanced	"We have multi-	4	4	Comprehensive	A few libraries

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
digital strategies (multi-location, cloud, cybersecurity)	location data backups and antivirus/firewall in place." "Cybersecurity and recovery frameworks are documented."			Digital Safeguards	demonstrate more robust and strategic digital preservation and recovery planning.
MIS or IT department manages digital protection	"Digital backups are handled by our MIS." "IT department is responsible for cybersecurity and documentation."	6	6	Delegated IT Oversight	Many libraries rely on external or institutional IT teams for maintaining digital security.

Challenges and Limitations Faced by Libraries in Developing and Implementing Comprehensive Risk Management Strategies

Table 2 highlights recurring challenges that hinder sustainable library planning, many of which stem from deep-seated issues of governance alignment and institutional priorities. A key analytic insight emerging across these findings is the structural decoupling between library operations and institutional quality assurance (QA) mechanisms. While participants consistently identified the Quality Assurance, Planning, and Development Office (QAPDO) as a potential enabler of resilience, its involvement in library risk management remains largely aspirational rather than operationalized.

This governance decoupling manifests in three critical ways, each amplifying the challenges reported. First, financial constraints—reported by all 15 participants—are not simply a budget shortfall, but a symptom of this disconnection. Investments in cybersecurity, digital preservation, and staff training are excluded from core institutional resource allocation because library resilience metrics are rarely linked to QA-driven performance indicators. This treats digital stewardship as a discretionary cost rather than an integral component of institutional quality.

Second, inadequate staff capacity and the need for strategic partnerships (12 responses each) further underscore this divide. When library staff lack training in cybersecurity or emergency response, it reflects a QA framework focused on accreditation compliance rather than continuous risk capacity-building. The expressed need for external partnerships highlights libraries attempting to compensate for internal governance gaps where support should be institutionally mandated and resourced.

Third, technological vulnerabilities (11 responses) and unstructured backup practices (8 responses) reveal a consequential tension and contradiction in institutional risk governance. Accountability for digital assets is frequently delegated to IT/MIS units without formal coordination, creating unclear ownership and conflicting priorities. While the institution depends on digital infrastructure, it often fails to provide consistent, secure, and modernized technological support to libraries, expecting protection without providing the tools or clear mandates.

Low prioritization and lack of formal plans (8 responses) are direct outcomes of both themes. When digital risk management is absent from institutional strategy, it exemplifies governance decoupling—libraries are sidelined in strategic QA processes. Simultaneously, it highlights a contradiction in risk governance: respondents acknowledge digital risk as a growing threat while describing it as a low institutional priority. This reflects an accountability gap rather than a knowledge deficit; libraries are constrained less by technical ignorance and more by governance structures that fail to translate awareness into institutional commitment.

Rather than indicating the absence of governance, the data point to a misalignment between existing QA authority and operational risk practices—supporting literature on symbolic compliance and loose coupling in higher education. The recurring call for support and partnerships indicates a strong willingness to improve, yet this motivation coexists with persistent constraints, revealing a system at odds with itself.

Overall, these challenges are not merely operational but are symptoms of systemic governance issues. The interlinked barriers reflect a cycle where decoupling from central QA leads to under-resourcing, which is exacerbated by contradictory institutional expectations around risk. This extends the findings of scholars like Šaparnienė et al. (2024) by framing constraints as outcomes of misaligned structures and conflicting institutional logics. Addressing these challenges, therefore, requires re-coupling library resilience with QA mechanisms—aligning budgets, mandates, and metrics—and resolving governance tensions through explicit policy integration and accountable, cross-functional coordination.

Table 2. Governance Decoupling Between Libraries and Institutional Quality Assurance and Tensions and Contradictions in Institutional Risk Governance

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
Low prioritization / lack of formal plan	"These have been suggested to our head Librarian but the priority as of now is not this." "There's no existing written policy yet." "We don't have a formal disaster plan."	8	8	Lack of Institutional Priority & Policy Framework	Risk management for digital collections is not a priority in some libraries, often due to lack of leadership attention, formal documentation, or institutional mandates.
Budget limitations	"Lack of budget." "Limited funding for tools, training, and digital infrastructure."	15	15	Financial Constraints	Inadequate financial support is the most cited issue, preventing investments in software, secure storage, and

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
	"Library budget constraints."				professional development.
Inadequate training / technical skills	"We need more training in cybersecurity." "Limited staff expertise in digital preservation." "Most staff are not trained in emergency response."	12	12	Lack of Staff Capacity	A shortage of skilled personnel trained in digital risk management, cybersecurity, and recovery processes hinders effective planning and implementation.
Cybersecurity and software vulnerabilities	"Cybersecurity is a major concern." "We are vulnerable to ransomware and phishing." "Software failure due to reliance on third-party or free tools."	11	11	Technological Vulnerabilities	Libraries feel exposed to increasing cyber threats and system failures due to limited infrastructure, outdated software, or weak security systems.
Weak or informal data backup systems	"We use USB drives and Google Drive manually." "Backups are not automated or tested." "No structured recovery protocol."	8	8	Unstructured Backup and Recovery Practices	While most libraries back up data, the lack of formal schedules, secure platforms, and recovery testing puts digital assets at risk.
Rapid tech changes / digital obsolescence	"Technology changes too fast." "Plans become outdated quickly due to evolving	5	5	Changing Digital Landscape	Libraries struggle to keep up with technological advancements and continuously evolving cyber threats, making

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
	threats."				long-term planning difficult.
Lack of coordination / support from other departments	"No collaboration with IT." "Library relies on MIS or external IT staff without formal involvement."	3	3	Weak Institutional Collaboration	Limited collaboration with IT and other support offices weakens the ability to design, update, or implement sustainable risk management plans.
Legal concerns and compliance issues	"Copyright issues." "No clear accountability for unsaved or lost files."	2	2	Legal and Ethical Challenges	Without legal clarity, libraries may unknowingly violate policies or suffer data loss without proper protection and recovery mechanisms.
Need for support, training, and partnerships	"We need staff seminars and cyber training." "More funding and collaboration with government or consortia." "MOA and benchmarking would help."	12	12	Call for Strategic Support and Partnerships	Libraries need institutional and external support—funding, policy guidance, staff training, and collaboration—to address their limitations and strengthen digital risk management.

The findings also reveal important tensions within institutional risk governance. While libraries express a strong willingness to improve preparedness, this motivation coexists with persistent constraints—limited budgets, insufficient training, and unclear mandates (Table 2). Notably, respondents simultaneously acknowledge digital risk as a growing threat while describing it as a low institutional priority, revealing a contradiction between risk awareness and strategic action.

This tension reflects an accountability gap rather than a knowledge deficit, suggesting that libraries are constrained less by technical ignorance and more by governance structures that fail to

translate awareness into institutional commitment (Rahmani, 2025; Šaparnienė et al., 2024). Without explicit policy mandates or QA-driven performance requirements, digital resilience remains discretionary rather than obligatory.

Role of QAPDO in Supporting Risk Preparedness and Resilience Planning for Library Operations

Table 3 reveals that library staff perceive the Quality Assurance, Planning, and Development Office (QAPDO) not merely as a support unit but as a critical source of institutional leverage, capable of elevating risk management from a library-specific concern to a strategic governance priority. Its unique position at the intersection of quality assurance, strategic planning, and accreditation grants QAPDO authority to recouple library operations with core institutional systems, transforming discretionary resilience efforts into governed practices. This potential is evident in three key areas.

First, QAPDO's mandate in strategic planning and accreditation enables it to translate compliance requirements into formalized risk management and contingency frameworks. By embedding digital resilience metrics and disaster recovery protocols into quality assurance cycles, ad hoc library practices can become auditable components of institutional governance.

Second, the office's role in staff training, capacity building, and resource mobilization positions it as a broker of cross-institutional support. Rather than libraries navigating challenges in isolation, QAPDO can coordinate funding, orchestrate inter-departmental training, and align human and technical resources, addressing capacity gaps and reducing fragmentation.

Third, expectations for performance monitoring and institutional alignment highlight QAPDO's capacity to institutionalize accountability. By creating feedback loops between libraries and central administration, the office bridges the gap between risk awareness and strategic action.

This perception aligns with broader evidence emphasizing that foundational governance structures enhance risk visibility across organizations (Germany et al., 2025) and echoes Jesry et al. 's (2022) argument for embedding risk mitigation within quality systems. QAPDO thus functions as a leverage point where policy, coordination, and oversight converge to systematically elevate the institution's risk governance maturity, resolve contradictory priorities, and integrate fragmented resilience practices into a coherent, institution-wide framework.

Table 3. Perceived QAPDO Role as Governance Leverage

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
General Role Recognition of QAPDO	"QAP ensures quality standards, supports planning and development, and leads accreditation and continuous improvement efforts."	10	10	Understanding of QAPDO Role	QAPDO is generally recognized as responsible for quality assurance, strategic planning, and institutional development.

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
QAPDO Contribution to Strategic Planning	"Yes, QAP has supported the library in strategic planning and aligning our goals with institutional priorities."	8	8	Strategic Involvement	QAPDO has contributed in aligning library plans with institutional goals and supporting accreditation processes.
Training and Capacity Building	"They could provide staff training on disaster preparedness, cybersecurity, and data protection."	9	9	Need for Staff Training	Staff training and seminars on disaster readiness and digital risk management are frequently requested.
Assistance in Risk Management & Contingency Planning	"QAPDO can help develop formal risk management and disaster recovery plans aligned with school policies."	10	10	Risk Planning Support	QAPDO is seen as capable of initiating and supporting risk assessment and contingency planning for libraries.
Policy and Documentation Development	"They can assist in drafting contingency plans and operational guidelines."	5	5	Policy Support	Libraries need help in crafting formal policies, operational procedures, and guidelines for preparedness.
Monitoring, Evaluation, and Alignment	"They monitor and align performance with institutional goals and quality standards."	6	6	Performance Monitoring	QAPDO's role includes aligning unit-level practices with institutional benchmarks and ensuring accountability.

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
Support in Resource Allocation	"They can help secure funding and tools needed for risk preparedness."	7	7	Support in Budget and Tools	Libraries request QAPDO's help in securing budget, resources, and tools needed for effective risk management.

Strategies, Tools, or Institutional Mechanisms that can be Adopted

The challenges and limitations identified in this study underscore the need to reconceptualize the library's role in institutional risk management. Digital resilience should be framed not as library-specific IT projects, but as a core component of institutional governance capacity—encompassing structures, policies, resources, and cultural norms that enable organizations to maintain operations amid digital disruption (Table 4).

Staff training and awareness, the most frequently cited priority, establishes the foundation of this governance capacity. Cross-training and cybersecurity workshops cultivate a risk-aware culture, positioning staff as primary agents of resilience rather than passive tool users. Technical measures—cloud storage, backups, and cybersecurity protocols—serve governance functions by safeguarding institutional assets and ensuring continuity of research and teaching missions.

Formal disaster recovery planning and policy integration transform ad-hoc responses into accountable, predictable processes, embedding resilience into university operations. Dedicated resource allocation and cross-functional collaboration further reinforce that resilience is a strategic, institution-wide investment rather than a siloed cost. Supporting strategies, including remote access, technology foresight, and evaluation mechanisms, enhance adaptive, user-centered, and forward-looking governance capacity.

Overall, these findings present a model that shifts digital resilience from a technical or departmental concern to a governance imperative. Aligning with Chigwada and Ngulube (2025), the study emphasizes proactive, collaborative preparedness, extending their work by positioning these measures as essential to modern universities' governance in a digitally complex, risk-prone environment.

Table 4. Reframing Digital Resilience as Governance Capacity

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
Cloud Storage and Backup Systems	"Cloud storage and cybersecurity protocols", "Regular cloud-based backups to secure digital collections", "Google Drive", "bigger server",	21	21	Cloud-based Digital Resilience	Libraries consistently emphasized the need for cloud-based storage and automated backup systems to protect digital collections and ensure continuity

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
	"secure cloud-based backups"				during disruptions.
Cybersecurity Protocols	"Cybersecurity protocols like MFA", "cybersecurity training", "antivirus software", "encryption and multi-factor authentication"	18	18	Cybersecurity Measures	Cybersecurity is a central concern, with calls for stronger protocols, staff training, and software tools to protect digital assets from evolving threats.
Remote Access Solutions	"Remote access", "virtual reference service", "digital lending", "offline editing and upload", "secure remote access"	12	12	Remote Service Accessibility	Ensuring continued access to services remotely during crises was a recurring strategy, including remote logins, virtual services, and online learning systems.
Disaster Recovery and Continuity Planning	"Disaster recovery plans", "risk and emergency plan", "business continuity plan", "recovery and restoration strategies"	17	17	Formal Risk and Recovery Planning	Libraries need to formalize disaster recovery strategies, with QAPDO support, to ensure swift service restoration after disruptions.
Staff Training and Awareness	"Trainings and seminars", "staff cross-training", "cybersecurity training", "technology workshops"	22	22	Staff Capacity Building	Regular training programs were identified as essential to keeping staff prepared for disruptions and abreast of new digital threats and

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
					tools.
Institutional Policies and Protocols	"Institutional policies", "risk preparedness plan", "disaster preparedness and response plan", "formal documentation", "asset assessment policies"	16	16	Institutional Policy Integration	Libraries called for institutionalized risk, disaster, and digital collection policies to be implemented in coordination with QAPDO.
Collaboration and Communication	"Collaboration with IT and QAPDO", "open communication with PQA", "cross-department engagement", "inter-office collaboration"	11	11	Collaborative Planning Approach	A multi-stakeholder collaboration model was suggested, involving QAPDO, IT, and administrative units to co-create and monitor digital resilience frameworks.
Resource Allocation and Infrastructure Support	"Emergency funding", "bigger server", "supporting the plans and budget", "technical support access", "allocate resources"	13	13	Institutional Resource Support	Participants highlighted the importance of budget, infrastructure, and IT resources—facilitated or endorsed by QAPDO—for successful risk management and resilience.
Technology Foresight and Innovation	"Adoption of emerging technologies", "tech foresight",	9	9	Keeping Up with Technological Changes	There was a recognized need for QAPDO to help libraries stay

Codes/Categories	Verbatim Responses	No. It Occurs	No. Of Participants Who Responded	Themes	Description Of Themes
	"updating systems", "innovation support"				current with digital trends and integrate new technologies in a structured way.
Evaluation and Feedback Mechanisms	"Post-incident review", "assess their response", "monitor implementation", "continuous improvement"	8	8	Continuous Evaluation & Improvement	Libraries stressed that digital resilience strategies must be dynamic, incorporating feedback and performance reviews to improve future response effectiveness.

Overall, the findings present a comprehensive perspective on the tools and approaches libraries consider essential for digital resilience: staff capacity building, cloud-based infrastructure, cybersecurity, formalized planning, institutional policies, cross-functional collaboration, and adequate resources. These strategies align with Chigwada and Ngulube (2025), who underscore proactive disaster preparedness—including risk assessment, staff training, digital preservation, and inter-organizational collaboration—as critical to sustaining library operations amid diverse threats.

Together, the findings position QAPDO as a central enabler of resilient, future-ready libraries, capable of coordinating policy development, resource mobilization, staff training, and strategic planning across institutional units. By championing these initiatives, QAPDO can help embed resilience into institutional practices, ensuring service continuity and long-term sustainability.

Proposed Action Plan: Library Risk Management and Digital Resilience with QAPDO Support

The proposed strategic action plan (Table 5) is not a generic set of recommendations, but a direct institutional response to the governance gaps identified in this study. It is explicitly derived from the core analytic themes, translating evidence into strategy: the fragmented preparedness observed informs the push for formal disaster recovery plans; the governance decoupling between QA and library operations motivates the creation of a cross-functional task force; the perceived leverage of QAPDO justifies integrating risk indicators into accreditation monitoring; and the accountability gaps underpin mandates for policy, training, and aligned budgets.

This approach reinforces the study's central thesis: digital resilience is fundamentally a governance challenge. As Park and Choi (2025) and Trembach (2024) argue, resilience emerges from the alignment of authority, accountability, and learning—not merely from technology. The action plan operationalizes this insight by positioning QAPDO as the key mechanism to convert awareness into obligation. Through its roles in policy alignment, compliance enforcement, resource

leverage, and performance monitoring, QAPDO can systematically elevate risk management from a discretionary library activity to an institutional governance function.

Therefore, the plan's ten goals—from establishing continuity plans and cybersecurity protocols to forming a QAPDO–Library–IT task force and embedding continuous evaluation—collectively represent a blueprint for maturing institutional capability. By bridging strategic vision and operational execution, QAPDO can help close the persistent gap between risk awareness and effective preparedness, fostering a culture of resilience that is structured, accountable, and sustained. This aligns with findings like those of Stanwicks (2024) on collaborative planning and moves beyond appeals for "support" to demonstrate how governance structures themselves determine resilience outcomes.

Table 5. Library Risk Management and Digital Resilience with QAPDO Support

Goal	Action Steps	Responsible Units	Timeline	Expected Outcome
1. Establish a Comprehensive Disaster Recovery and Continuity Plan	- Draft formal risk management and disaster recovery policies - Align library continuity plan with institutional DRP and QAPDO's quality standards	Library, QAPDO, IT Office	Q4 2025	Approved and documented risk and recovery plan for the library
2. Enhance Cybersecurity Protocols	- Conduct cybersecurity audit - Implement MFA, antivirus, and data encryption solutions - Create SOPs for digital threats	Library, QAPDO, IT Office	Q4 2025 – Q1 2026	Secure library systems and reduced digital vulnerabilities
3. Migrate to and Maintain Cloud-Based Backup Systems	- Identify suitable cloud service providers - Backup digital collections and key documents regularly - Test restoration protocols	Library, QAPDO, IT Office, Finance	Q1 2026	Reliable and accessible cloud storage system for critical digital content
4. Ensure Remote Service Accessibility	- Develop remote login for staff and students - Implement virtual reference and lending systems	Library, QAPDO, IT Office	Q1 2026	Continuity of library services during disruptions

	- Integrate remote services into DRP			
5. Build Staff Capacity Through Continuous Training	- Develop a training calendar - Conduct workshops on cybersecurity, risk response, cloud systems, and digital safety	QAPDO, Library, HR	Q4 2025 – ongoing	Informed and proactive library staff prepared for digital and operational disruptions
7. Establish a Technology Monitoring and Innovation Desk	- QAPDO to track emerging technologies and trends - Recommend updates/upgrades for library systems - Hold quarterly innovation briefings	QAPDO, Library, IT	Q1 2026 – ongoing	Proactive adoption of emerging technologies
8. Formalize Interdepartmental Collaboration	- Create a QAPDO–Library–IT–GSO task force - Develop a shared digital resilience roadmap - Schedule biannual coordination meetings	QAPDO, Library, IT, GSO	Q4 2025 – ongoing	Strengthened inter-office synergy for risk prevention and response
9. Secure Resource Allocation and Infrastructure Support	- QAPDO to endorse budget proposals - Request for emergency funding allocation - Invest in larger servers and reliable digital tools	QAPDO, Library, Budget Office	Q1 2026 – Q2 2026	Sustained funding and IT infrastructure for digital resilience
10. Implement Continuous Evaluation and Feedback Mechanisms	- Conduct post-incident reviews - Monitor KPIs on response time, downtime, and staff readiness	QAPDO, Library	Q2 2026 – ongoing	Continuous improvement of resilience planning and system efficiency

	- Incorporate feedback into improved risk planning

CONCLUSIONS

The findings show that although academic libraries have adopted minimum, compliance-driven risk measures such as fire protection and manual data backups, these practices remain fragmented, reactive, and inadequate for managing complex digital risks. Persistent gaps in formal disaster recovery planning, cybersecurity governance, staff capacity development, and policy integration—especially for digital collections—reflect governance misalignment rather than mere operational weakness.

A key contribution of this study is identifying governance decoupling between library operations and institutional quality assurance systems as the central barrier to sustainable digital resilience. While awareness of digital risk is high, accountability and strategic prioritization remain low, indicating an institutional accountability gap rather than a lack of technical knowledge.

The study further establishes the Quality Assurance, Planning, and Development Office (QAPDO) as a governance leverage point, capable of re-coupling fragmented library practices with institutional planning, policy development, accreditation-linked monitoring, capacity-building, and resource allocation. When strategically activated, QAPDO can transform digital resilience from a discretionary activity into a governed institutional obligation.

The proposed action plan operationalizes this shift by embedding disaster recovery, cybersecurity, cloud infrastructure, staff development, and cross-functional coordination within QAPDO-led quality assurance processes. This reframes digital resilience from isolated technical solutions to an institutional governance capability, ensuring continuity, accountability, and adaptability.

Overall, the study affirms that digital resilience in academic libraries is fundamentally a governance challenge, and that embedding risk management within quality assurance systems is essential for developing future-ready, resilient higher education institutions.

LIMITATION & FURTHER RESEARCH

This study has several limitations that constrain the interpretation of its findings. First, results are based on self-reported accounts from 20 library personnel, reflecting perceived risk preparedness and governance support rather than independently verified institutional conditions. Consequently, the study cannot confirm the effectiveness, maturity, or technical adequacy of disaster recovery plans, cybersecurity measures, or digital risk protocols.

Second, the study did not include technical audits, system testing, or on-site assessments. Identified gaps should therefore be understood as governance- and planning-level deficiencies, not definitive evaluations of operational compliance or system security. Third, the bounded qualitative case design limits generalizability; findings are analytically applicable to higher education institutions with formal quality assurance structures, but not sector-wide.

Future research should adopt mixed-methods approaches that combine qualitative governance analysis with technical audits, disaster recovery simulations, and longitudinal evaluation. Comparative studies involving diverse stakeholders, including IT leaders and senior administrators, would clarify how governance structures shape institutional digital resilience.

REFERENCES

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation

for novice researchers. *The Qualitative Report, 13*(4), 544–559. https://doi.org/10.46743/2160-3715/2008.1573

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Brown, H. (2021). Interconnected disaster management: Bridging the physical and digital divide. *Journal of the Australian Library and Information Association, 70*(3), 263–286. https://doi.org/10.1080/24750158.2021.1958464

Chigwada, J., & Ngulube, P. (2025). Disaster preparedness and management practices in academic libraries in context. *International Journal of Disaster Management, 7*(3), 261–283. https://doi.org/10.24815/ijdm.v7i3.40580

Cox, J. (2020). The higher education environment driving academic library strategy: A political, economic, social and technological (PEST) analysis. *The Journal of Academic Librarianship, 47*(1), 102219. https://doi.org/10.1016/j.acalib.2020.102219

Cox, J. (2023). The position and prospects of academic libraries: Weaknesses, threats and proposed strategic directions. *New Review of Academic Librarianship, 29*(3), 263–287. https://doi.org/10.1080/13614533.2023.2238691

Dada, K. S. J., Hamza, J. M., & Mohammed, H. A. (2025). Disaster risk management in libraries and information centers: Global strategies, challenges, policy and recommendations. *International Journal of Disaster Risk Management, 7*(1), 203–214. https://doi.org/10.18485/ijdrm.2025.7.1.11

Edward, A., Dodzi, O. F., & Wilson, A. B. K. (2025). Ensuring disaster management practices in academic libraries of Ghana: The issues at hand. *International Journal of Disaster Risk Management, 7*(1), 399–416. https://doi.org/10.18485/ijdrm.2025.7.1.23

Ganesamoorthy, M., & Selvakamal, P. (2024). Emerging technologies and trends in library: A study. In *Proceedings of the conference connecting the nations for knowledge and cultural heritage* (Puducherry). https://www.researchgate.net/publication/378183766

Garnett, J. (2019). Academic libraries: Changing the approach—Resilience building against disruptive events and the contribution to disaster risk reduction frameworks. *New Review of Academic Librarianship, 27*(1), 113–129. https://doi.org/10.1080/13614533.2019.1703767

Gbotosho, A. S., & Opele, J. K. (2025). Best practices for developing and maintaining digital libraries: An explorative study. *Journal of Applied Information Science and Technology, 18*(1), 123–130.

George, E. S., & Wagwu, V. (2025). The evolving roles of academic libraries in the 21st century: Opportunities and challenges. *International Journal of Social Sciences and Management Research*. https://doi.org/10.56201/ijssmr.vol.11no4.2025.pg487.498

Germany, I. R., Babatunde, L. A., Ajayi, J. O., Erigh, E. D., Obuse, E., Essien, I. A., & Ayanbode, N. (2025). Designing foundational governance structures for organizational risk visibility: A systematic review. *Engineering and Technology Journal, 10*(9). https://doi.org/10.47191/etj/v10i09.16

Hamad, F. (2023). Libraries' roles and practices to enhance information resilience: Academic librarians' perspectives. *Journal of Information Science*. https://doi.org/10.1177/01655515231191226

Hennink, M., & Kaiser, B. N. (2021). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine, 292*, 114523. https://doi.org/10.1016/j.socscimed.2021.114523

Hoving, S. (2025, March 11). Future-proofing academic librarians with essential skills and leadership. *Springer Nature*. Retrieved July 9, 2025, from

https://www.springernature.com/gp/librarians/the-link/research-management-blogpost/librarian-skills-future-preparing-for-challenges/27742188

International Organization for Standardization. (2015). *ISO 9001:2015 quality management systems—Requirements*.

Jesry, M., Omar, F. A., Rashwani, A., Bark, I., Jammo, K., Ajam, S., & Kassab, Z. (2022). Exploring the value of a risk-management quality-assurance model to support delivery of quality higher education in the conflict-affected northwest of Syria. *International Journal of Educational Research Open, 3*, 100134. https://doi.org/10.1016/j.ijedro.2022.100134

Koutsochera, D. (2025, November 13). From compliance gatekeepers to strategic enablers of excellence. *CQI*. Retrieved January 15, 2026, from https://www.quality.org/article/compliance-gatekeepers-strategic-enablers-excellence

Lee, P. (2025). Navigating the path to sustainability: Digital resilience in libraries. *IFLA Journal*. https://doi.org/10.1177/03400352251331465

Mozaffari, A., Hayati, Z., & Mozaffari, E. (2019). Applying risk management and prioritizing risks to enhance the performance of public library librarians in Fars Province. *Library and Information Science Studies*. https://doi.org/10.22055/slis.2019.18386.1247

Nicholas, P., Palmer, A., Lindsay, Y., Lawrence, K., & Lawson, V. L. R. (2023). Future proofing the academic library: Improving the way we work. *Library Hi Tech News, 40*(10), 14–16. https://doi.org/10.1108/lhtn-02-2023-0026

Opele, J. K. (2021). The impact of emerging technologies on library education: A global perspective. *Journal of Library and Information Science, 6*(2). https://journals.ui.edu.ng/index.php/uijlis/article/download/1378/1102/3839

Park, M. J., & Choi, H. (2025). Bending, not breaking: Digital resilience as a pathway to transformative renewal. *Technology in Society, 84*, 103138. https://doi.org/10.1016/j.techsoc.2025.103138

Rahmani, M. (2025). Strategic risk management in public library services: Approaches to prioritization and mitigation. *Malaysian Journal of Library & Information Science, 30*(1), 78–111. https://doi.org/10.22452/mjlis.vol30no1.4

Šaparnienė, D., Kulikauskienė, K., Aleksandravičiūtė, N., & Miežinienė, V. (2024). Challenges in managing public library services aimed at ensuring the well-being of society in the context of emergency situations. *Social Welfare: Interdisciplinary Approach, 14*, 115–133. https://doi.org/10.15388/sw.2024.14.8

Silliman University Library System. (2023, January 18). Transforming libraries for the digital age: Navigating the challenges. https://www.sulibraryph.com/blog/transforming-libraries-for-the-digital-age/transforming-libraries-for-the-digital-age

Stanwicks, K. N. (2024). From SWOT to success: The collaborative strategic planning journey of an academic library department. *Library Leadership and Management, 37*(3), 1–21.

Trembach, S. (2024). Thrive in an age of uncertainty? Using the ADAPT framework to build resilient academic libraries. *Kansas Library Association College and University Libraries Section Proceedings, 14*(1). https://doi.org/10.4148/2160-942x.1100