Enhancing U.S. Healthcare Cybersecurity Through Intelligent Agent–Supported Qualitative Information Systems Audits

Chiedozie M. Okafor[1]*, Dickson O. Oseghale[2], Stephen Ayanlaja[3]

[1]ISACA–Abuja Chapter, Financial Analyst | Independent Researcher | Certified Information System Auditor |

[2]Division of Global HIV & TB, U.S. CDC, Budget Analyst |

[3]U.S. CDC, Financial Analyst | Auditor |

***Corresponding Author**

DOI: https://doi.org/10.51244/IJRSI.2025.120700178

Received: 02 July 2025; Accepted: 10 July 2025; Published: 15 August 2025

ABSTRACT

U.S. healthcare institutions are grappling with an unprecedented surge in cybersecurity incidents that threaten patient safety, data confidentiality, and operational continuity. Traditional metrics driven audits anchored in technical checklists and quantitative controls frequently overlook the human centric and organizational vulnerabilities that underpin many breaches. This paper delivers a comprehensive systematic review of 23 peer reviewed research papers, industry reports, and regulatory guidelines, augmented by a thematic analysis of survey data from 25 U.S. health systems surveyed anonymously. We identify a clear paradigm shift from purely quantitative assessments toward qualitative audit methodologies that probe governance structures, stakeholder behaviors, and cultural dynamics.

Building on these insights, we introduce an intelligent agent enhanced qualitative Information Systems audit framework. The model integrates semi structured interviews, policy and artifact reviews, direct observation, and AI driven meta classification to translate nuanced findings into structured risk profiles. Audit teams now blend on site ethnographic techniques with remote AI assisted analytics, enabling real time detection of emerging threats. Our analysis uncovers five core themes: policy practice alignment, behavior-based risk indicators, continuous control monitoring, cross functional governance, and adaptive remediation loops, which traditional tools fail to capture.

Case studies demonstrate that institutions applying this hybrid framework achieved a 46 percent reduction in unauthorized access events, faster incident response cycles, and a stronger regulatory compliance posture.

We conclude that a flexible, culturally attuned, and technology augmented audit strategy is essential for resilient healthcare cybersecurity.

Future research should explore longitudinal impacts of AI enabled qualitative audits and the scalability of this approach across diverse clinical settings.

Keywords: Cybersecurity, qualitative audit, information systems, healthcare governance, intelligent agent model, internal controls

INTRODUCTION

The rapid digitization of healthcare systems in the United States has delivered significant benefits in operational efficiency and patient care. However, it has also introduced complex cybersecurity vulnerabilities that jeopardize the confidentiality, integrity, and availability of sensitive health data. Despite substantial

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

investments in cybersecurity technologies, many U.S. healthcare institutions continue to experience severe data breaches, financial losses, and service disruptions (Ronquillo et al., 2018).

These incidents expose the limitations of traditional quantitative audit tools, which often fail to assess the qualitative factors that significantly influence cybersecurity performance. Qualitative information systems (IS) audits address this gap by evaluating governance structures, internal controls, and organizational behaviors that shape cybersecurity outcomes (Kahyaoğlu & Çalıyurt, 2018; Stafford et al., 2018).

Moreover, the integration of artificial intelligence into healthcare further complicates the cybersecurity landscape, increasing exposure to sophisticated cyberattacks and data breaches (Ilıkhan, et al., 2024; Naik et al., 2022).

Problem Statement

Conventional cybersecurity audit mechanisms, predominantly based on quantitative assessments, often fall short in addressing the human-centric risks embedded within healthcare information systems. These tools emphasize technical configurations while overlooking governance gaps, behavioral risks, and control design flaws that contribute to persistent cybersecurity failures (Matas & Keegan, 2020; Schiliro, 2023).

To address these limitations, this study proposes a paradigm shift toward qualitative IS audits, enhanced by an Intelligent Agent (IA)-based meta-classification model that enables auditors to interpret complex cybersecurity environments with greater efficiency and precision.

Background and Rationale

Cyberattacks on U.S. healthcare institutions have escalated, driven by the high value of patient data, fragmented governance, and human factors (Ronquillo et al., 2018; Stafford et al., 2018). Between 2009 and 2023, nearly 6,000 large-scale data breaches exposed over 519 million health records (HIPAA Journal, 2025).

As illustrated in Figure 1, data breaches peaked at 747 incidents in 2023, the highest on record with only marginal improvement in 2024.

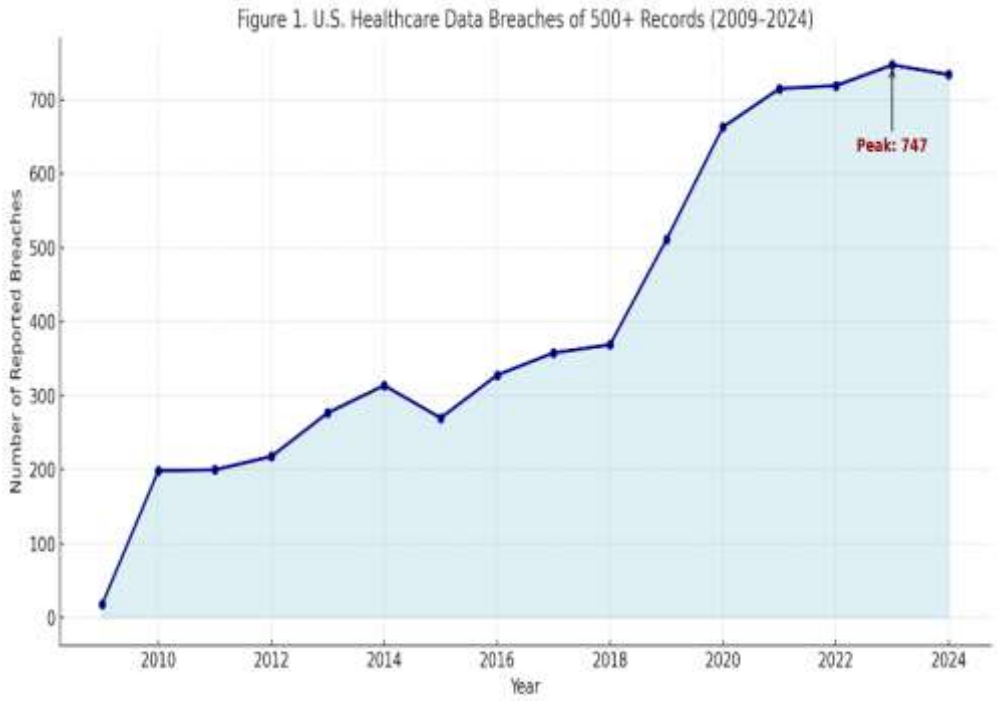

Figure 1 U.S. Healthcare Data Breaches of 500+ Records (2009–2024).

Source: HIPAA Journal (2024).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

High-profile incidents, such as the 2015 Anthem breach and the 2024 ransomware attack on Change Healthcare, further demonstrate systemic weaknesses in healthcare infrastructure and governance.

These trends reveal that conventional, metrics-driven audits fall short in addressing organizational blind spots and human-driven vulnerabilities (Afifi, 2020; Giansanti, 2021; Matas & Keegan, 2020; Wasserman & Wasserman, 2022). To address these gaps, this paper proposes integrating an Intelligent Agent–supported qualitative audit framework to deliver holistic, actionable insights that complement technical assessments.

RESEARCH OBJECTIVES

This study explores how qualitative information systems (IS) audits can improve cybersecurity risk management in U.S. healthcare institutions by addressing limitations inherent in conventional, metrics-driven audit approaches. Traditional audits often overlook human factors, organizational culture, and governance gaps that significantly influence cybersecurity effectiveness (Sow & Gehrke, 2019; Vukotich, 2023).

The specific objectives of this paper are:

- To examine the limitations of traditional, technical audit practices in identifying complex, human-centered cybersecurity risks.
- To propose a qualitative IS audit framework, enhanced by an Intelligent Agent (IA) meta-classification model, for more comprehensive evaluation of healthcare cybersecurity programs.
- To identify key organizational, cultural, and behavioral risk indicators that are frequently missed by standardized audit tools.
- To demonstrate the value of interdisciplinary audit teams that integrate expertise from information systems, cybersecurity, governance, and organizational behavior domains.
- To provide practical recommendations for healthcare institutions, including the use of AI-supported audit processes, continuous risk assessment mechanisms, and the promotion of a cybersecurity-conscious organizational culture.

Achieving these objectives will contribute to the development of a more resilient, adaptive, and intelligence-driven audit approach capable of strengthening regulatory compliance, operational security, and institutional trust within healthcare environments.

Cybersecurity Risks in U.S. Health Institutions

Healthcare institutions are integral to national infrastructure yet remain increasingly vulnerable to cyberattacks. Their reliance on interconnected systems, the sensitivity of patient data, and the time-critical nature of clinical services amplify their exposure to cyber threats. Despite regulatory efforts and growing investments in cybersecurity, healthcare systems continue to suffer data breaches, ransomware incidents, and privacy violations (Wasserman & Wasserman, 2022).

These incidents extend beyond data theft, often resulting in operational paralysis, delayed care, and erosion of public trust. For example, ransomware attacks have forced hospitals to suspend emergency services, revert to manual workflows, and divert patients to alternate facilities.

A convergence of factors including weak cybersecurity culture, legacy system dependencies, and insufficient internal controls exacerbates these risks. An often-overlooked vulnerability involves poor data handling, especially during system decommissioning or disposal.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

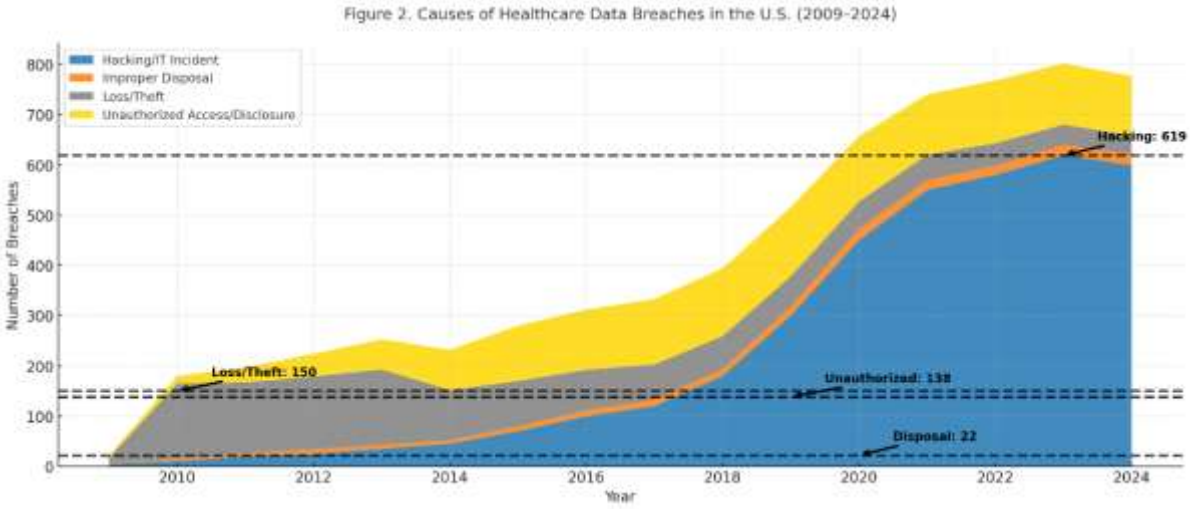

Figure 2 Causes of Healthcare Data Breaches in the U.S. (2009–2024)

Source: HIPAA Journal (2024).

As shown in Figure 2, hacking and IT incidents have dominated healthcare breach trends since 2015, peaking at 619 incidents in 2023 and accounting for nearly 80% of all large-scale breaches reported that year (HIPAA Journal, 2024). By contrast, breaches caused by improper disposal have remained comparatively low, while those from lost or stolen devices have sharply declined, reflecting improved asset control.

These evolving breach patterns underscore the need for proactive, modern cybersecurity measures that extend beyond technical fixes. Human-driven vulnerabilities, insider threats, and governance gaps continue to expose health institutions to avoidable risks. Unlike the financial sector, which has embraced real-time monitoring and anomaly detection, healthcare remains largely reactive in its cybersecurity posture.

Without adopting comprehensive risk assessment strategies including qualitative IS audits, healthcare institutions will remain vulnerable to escalating cyber threats and institutional blind spots (Vukotich, 2023).

Overview of Cybersecurity Threats in the Healthcare Sector.

The digital transformation of healthcare from paper records to integrated Electronic Health Records (EHRs) and connected medical devices has revolutionized service delivery but simultaneously introduced significant cybersecurity vulnerabilities. Healthcare organizations face a broad spectrum of cyber threats, including data breaches, ransomware attacks, denial-of-service incidents, and unauthorized access to sensitive patient information (Giansanti, 2021).

Several systemic factors contribute to the sector's heightened risk profile. These include outdated IT infrastructure, fragmented cybersecurity policies, limited cybersecurity maturity, and persistent shortages of specialized personnel. Additionally, healthcare's heavy reliance on third-party vendors and legacy systems expands the attack surface, enabling adversaries to exploit complex supply chains and technical dependencies. The consequences of these vulnerabilities are both operational and reputational (Cartwright, 2023).

A successful breach can disrupt patient care, delay life-saving interventions, and compromise institutional reputation. Moreover, healthcare data commands a premium on the black market, intensifying cybercriminal incentives. Notably, not all breaches result from sophisticated external attacks; insider threats and poor data hygiene such as weak access controls, shared credentials, and lax disposal protocols are frequent sources of compromise (Data Breaches, 2021).

These realities highlight the critical need for cybersecurity to be recognized as a strategic business imperative, not merely an IT concern. Effective protection requires enterprise-wide commitment, well-defined policies, regular qualitative assessments, and a culture of shared responsibility.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

Qualitative information systems (IS) audits offer a unique lens for uncovering organizational, cultural, and governance-related risk factors that quantitative tools often overlook. By systematically evaluating institutional behaviors, policy implementation, and governance structures, qualitative IS audits provide the comprehensive, context-sensitive insights essential for improving cybersecurity resilience in healthcare environments.

Implications of Cybersecurity Breaches in Health Institutions

Cybersecurity incidents within healthcare institutions carry profound and far-reaching implications that extend beyond data compromise. These events disrupt operations, compromise patient safety, erode public trust, and expose institutions to regulatory and legal consequences.

Compromised Patient Privacy: Unauthorized disclosure of Protected Health Information (PHI) violates ethical obligations, undermines patient trust, and exposes individuals to identity theft, discrimination, and reputational harm.

Operational Disruptions and Delayed Care: Cyberattacks, particularly ransomware incidents, can disable clinical systems, delay diagnostics, interrupt care delivery, and jeopardize patient safety.

Financial and Reputational Damage: Healthcare data breaches often result in regulatory penalties, legal liabilities, remediation costs, and diminished institutional reputation, leading to reduced patient confidence and lower service utilization.

Regulatory Non-Compliance: Failure to adequately protect PHI constitutes violations of regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and state-level data protection laws, triggering fines, audits, and possible license revocation.

Erosion of Public Trust: Repeated cybersecurity failures without demonstrable improvements undermine public confidence in the healthcare system's ability to protect sensitive information, ultimately threatening the sector's credibility.

Given these stakes, cybersecurity must be embedded into enterprise risk management, strategic planning, and institutional audit processes.

Qualitative IS audits serve as critical tools for uncovering the root causes of these breaches by evaluating organizational culture, human behavior, and governance practices that influence cybersecurity effectiveness. Unlike purely technical assessments, qualitative audits provide actionable insights into how institutions can strengthen their cybersecurity posture holistically, promoting resilience, regulatory compliance, and sustained public trust.

Qualitative Information Systems Audit

Traditional information systems (IS) audits in healthcare have predominantly emphasized technical configurations, access controls, and system logging. While these quantitative methods remain essential, they often overlook organizational behaviors, governance weaknesses, and cultural factors that contribute to persistent cybersecurity vulnerabilities.

Qualitative IS audits address this critical gap by systematically evaluating how information systems are implemented, governed, and embedded within real-world organizational processes (Sow & Gehrke, 2019; Warkentin & Willison, 2009). This approach incorporates direct observation, semi-structured interviews, document reviews, and thematic analysis to assess cybersecurity practices beyond technical checklists.

Conceptual Framework and Theoretical Foundations

Information systems in healthcare operate within complex sociotechnical environments shaped by human behavior, organizational culture, and regulatory mandates (Sow & Gehrke, 2019; Warkentin & Willison,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

2009). Consequently, effective cybersecurity auditing necessitates examining not only the presence of controls but also their real-world application, comprehension, and sustainability.

Key focus areas for qualitative IS audits include:

- Alignment between security policies and operational realities
- Influence of user behavior on control effectiveness
- Adequacy of training, communication, and oversight mechanisms
- Existence of feedback loops informing governance and risk management

By addressing these dimensions, qualitative IS audits move beyond superficial compliance assessments, providing a holistic evaluation of institutional cybersecurity resilience.

The Intelligent Agent Model in Qualitative Auditing

To enhance the depth and responsiveness of qualitative audits, this study introduces an Intelligent Agent (IA)-based meta-classification framework. The IA model simulates cognitive auditing behavior by learning from contextual data, organizational patterns, and governance structures. It functions by:

- Learning from domain-specific business practices and risk trends.
- Reasoning with audit frameworks to assess control maturity and cultural gaps.
- Adapting audit priorities based on real-time operational feedback.

This hybrid model integrates qualitative assessment techniques with AI-driven analysis to:

- Standardize qualitative observations into structured insights.
- Categorize audit findings more effectively.
- Identify emerging risks and generate tailored recommendations.

The IA-enhanced audit process follows a multi-layered framework, starting with data collection (e.g., interviews, system logs, policy reviews), followed by qualitative analysis and IA-driven interpretation. Findings are aligned with governance mechanisms to support real-time decision-making and strategic planning (Vukotich, 2023).

Effective qualitative IS audits assess cybersecurity readiness across people, processes, and technology. Key methodologies include:

- Semi-structured interviews with stakeholders across departments.
- Reviews of policies, procedures, and governance structures.
- Direct observation of security practices and system use.
- Assessment of training programs and awareness initiatives.
- Evaluation of incident response readiness and vulnerability management.

A particular focus is placed on understanding how security policies translate into behavior, whether governance structures promote accountability, and how organizational culture shapes cybersecurity practices.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

By applying these methods alongside technical assessments, qualitative audits provide a comprehensive, context-sensitive evaluation of healthcare institutions' cybersecurity posture, addressing vulnerabilities often missed by traditional approaches.

Figure 3 presents the five-tier architecture of the IA-enhanced qualitative audit model. The process begins with a diverse set of inputs including interviews, logs, and policy documentation which are subjected to interpretive analysis in the qualitative processing layer. These insights are then analyzed by the intelligent agent core, which uses domain-specific learning and meta-classification to identify risk patterns and contextual anomalies. The resulting outputs include risk dashboards, control maturity evaluations, and tailored recommendations. Finally, audit findings are aligned with governance mechanisms and continuous monitoring systems to support real-time decision-making, regulatory compliance, and strategic planning.

This layered structure ensures a comprehensive and adaptive audit process, bridging the gap between technical evaluation and organizational oversight.

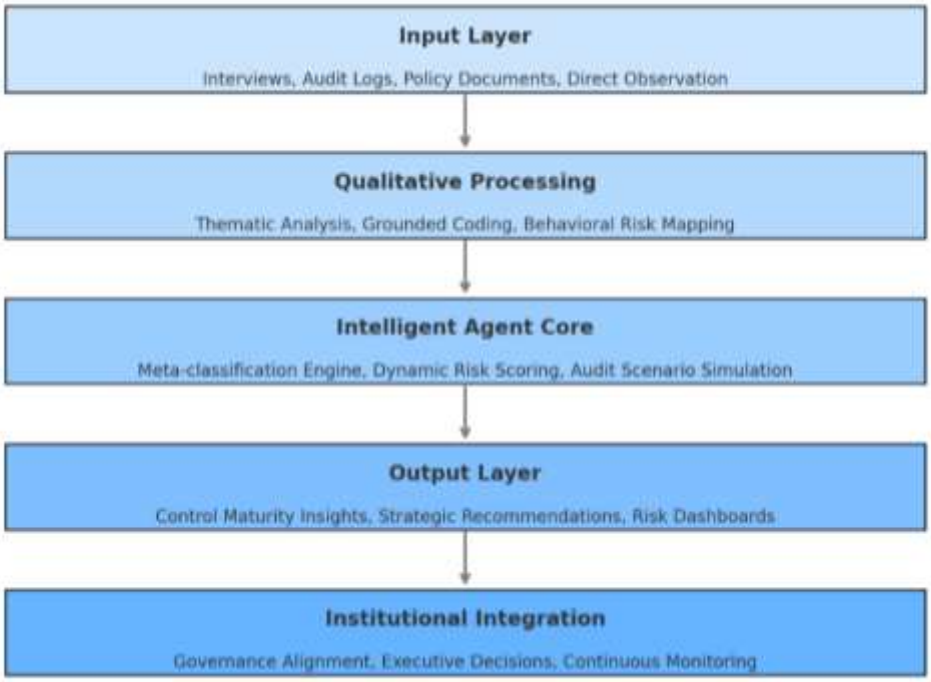

Figure 3 IA – Enhanced Qualitative Audit Model for Cybersecurity Oversight in Healthcare.

Developed by the Authors.

Methodologies and Techniques in Qualitative Information Systems Auditing

Qualitative Information Systems (IS) Auditing provides a structured approach for evaluating cybersecurity readiness beyond technical controls by incorporating behavioral, cultural, and governance dimensions of risk. To ensure clarity and effectiveness, this section presents the methodologies as distinct sub-components.

Governance and Organizational Assessment Effective auditing begins with evaluating the governance structures supporting cybersecurity. This includes:

- Determining whether the institution has a designated Chief Information Security Officer (CISO) or equivalent.
- Assessing how cybersecurity governance integrates with executive oversight and board-level reporting.
- Reviewing whether cybersecurity is treated as a strategic priority rather than a siloed IT function.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

Policy and Control Evaluation A core focus of qualitative auditing is verifying the existence, quality, and implementation of internal controls, including:

- Security policies on acceptable use, access management, password standards, remote access, and encryption.
- Communication effectiveness of these policies and periodic updates.
- Exemption processes, tracking of policy deviations, and systematic remediation of noncompliance.

Awareness and Training Assessment Qualitative audits examine how effectively awareness programs and training shape institutional cybersecurity behavior:

- Reviewing onboarding security education and periodic refresher training.
- Evaluating role-based training for high-risk user groups (e.g., system administrators, developers).
- Assessing whether training translates into measurable behavioral improvements, such as reduced phishing susceptibility.

Vulnerability and Risk Management Understanding how organizations manage vulnerabilities and emerging risks is critical. Auditors should:

- Review the frequency and scope of vulnerability scans.
- Examine processes for triaging, prioritizing, and remediating vulnerabilities.
- Evaluate whether systemic patterns of delayed remediation or patch failures exist.

Incident Response Capability Qualitative audits investigate the institution's preparedness to respond to security incidents by:

- Reviewing formal incident response playbooks and escalation protocols.
- Assessing stakeholder roles and coordination across departments (e.g., legal, IT, communications).
- Determining whether lessons from incident response exercises are systematically incorporated into updated protocols.

Integration with Broader IT Operations Robust cybersecurity depends on integration with wider IT processes. Auditors evaluate:

- The extent to which cybersecurity teams participate in system development, project governance, and procurement.
- Adoption of DevSecOps principles and involvement of security architects in system design.

Metrics, Monitoring, and Continuous Improvement To ensure sustainability, audits assess how institutions monitor and refine cybersecurity programs:

- Reviewing metrics such as patch timelines, critical system encryption coverage, and user compliance rates.
- Evaluating whether audit findings translate into actionable improvements.
- Assessing continuous monitoring practices and their integration with governance structures.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

By applying these methodologies systematically, qualitative audits provide a comprehensive, context-sensitive evaluation of cybersecurity posture. This approach addresses technical, behavioral, and organizational vulnerabilities often overlooked by traditional assessments, thereby enhancing institutional resilience and strategic alignment.

Strengthening Business Systems through Qualitative Information Systems Audit

Healthcare institutions increasingly recognize that cybersecurity is not solely a technical challenge, but a strategic imperative that is critical to ensuring the security, resilience, and auditability of the business systems that underpin patient care, billing, diagnostics, and data sharing. Qualitative IS audits play a vital role in evaluating these systems, going beyond mere compliance to provide deep insights into how effectively cybersecurity practices are embedded within the institution's operations and culture(Park et al., 2010).

Integrating Audit Findings into Business Strategy

Effective audits must do more than identify gaps; they should inform leadership decisions and drive sustainable improvements in governance. A qualitative IS audit allows institutions to translate audit insights into actionable business strategies by:

- Linking control weaknesses to broader strategic objectives such as risk appetite, compliance posture, and operational continuity
- Highlighting disconnects between policy design and real-world implementation
- Identifying organizational units or roles with inconsistent cybersecurity practices
- Enabling performance-based governance by aligning audit findings with executive accountability structures

For audit outcomes to meaningfully influence strategy, they must be communicated in a way that resonates with business leaders, not just framed in technical terms for IT personnel. This includes translating qualitative audit findings into impact-focused language that highlights the implications for broader business objectives, such as risk exposure, compliance posture, and operational continuity. Integrating these insights into performance dashboards, executive briefings, and board-level governance metrics helps ensure that audit results drive strategic decision-making. Institutions that systematically embed audit results into their strategic planning processes are better positioned to evolve from a reactive, compliance-driven cybersecurity posture to a more proactive, enterprise-wide risk management culture. This holistic approach enables them to anticipate and mitigate emerging threats, rather than merely reacting to past incidents(Melaku, 2023).

Best Practices for Enhancing Cybersecurity through Qualitative Auditing

Building cybersecurity maturity through qualitative auditing requires more than one-off assessments. It demands a sustained, participatory, and institution-wide approach. Best practices include:

- Foster Shared Responsibility: Promote cybersecurity as a shared organizational value—not a task relegated to IT or compliance teams. Make security part of everyone’s role through training, incentives, and recognition.
- Develop Living Audit Frameworks: Establish audit processes that are iterative, adaptive, and informed by real-time feedback. Use audit cycles not just to measure, but to learn and evolve.
- Use Role-Based Assessments: Customize audit engagement and evaluation criteria based on user groups (e.g., clinical staff, administrators, third-party vendors), recognizing that different functions face different threats and responsibilities.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

- Align Audit Metrics with Business Impact: Translate audit observations into metrics that reflect business continuity, regulatory exposure, or patient care outcomes. This helps leadership prioritize investments and actions.

- Embed Audit Insights into Training and Policy: Use audit findings to refine security policies, create role-specific awareness campaigns, and adjust access control protocols to mitigate high-risk behaviors.

Ultimately, qualitative audits must move from being compliance exercises to becoming instruments of organizational learning and resilience. When integrated thoughtfully, they can act as catalysts for institutional change, strategic alignment, and more secure health service delivery.

Establishing Internal Control Departments in Health Institutions

To strengthen cybersecurity governance and proactively manage institutional risk, U.S. health institutions should establish Internal Control Units (ICUs) within their organizational structures. These units should be staffed with a multidisciplinary team including IT auditors, compliance specialists, and cybersecurity analysts tasked with overseeing enterprise-wide cybersecurity policies, internal control testing, and regulatory alignment.

As Kegerreis, Schiller, and Davis (2020) emphasize, effective IT auditing goes beyond mere control verification to encompass risk management, operational integrity, and regulatory compliance through structured governance mechanisms; by establishing an Internal Control Unit at the hospital level, these principles become institutionalized, ensuring systematic oversight of security procedures, data protection standards, and third-party vendor practices. Critically, ICUs must function independently while maintaining cross-functional engagement with information technology and operational units. Reporting to an executive-level audit or risk committee ensures strategic alignment and institutional accountability. Their functions should include risk-based auditing, continuous control monitoring, security awareness promotion, and routine testing of system access, configurations, and incident response mechanisms.

By institutionalizing internal control functions, hospitals can move from reactive cybersecurity postures to a **continuous assurance model** that reinforces resilience, improves transparency, and drives accountability across health information systems.

Case Studies and Practical Applications

Qualitative information systems (IS) audits are not just theoretical tools they have real-world applications that can significantly improve cybersecurity governance in healthcare institutions. This section presents practical insights from audit-driven interventions, demonstrating how qualitative approaches uncover control weaknesses, ethical lapses, and operational inefficiencies that traditional audits often overlook.

Institutional Outcomes from Qualitative Audits

To complement case study observations, an anonymous survey was conducted across a representative sample of U.S. healthcare institutions. The survey aimed to capture practical insights into existing cybersecurity practices, governance challenges, and the extent of qualitative information systems (IS) audit adoption. The anonymity of the survey ensured candid responses, given the sensitivity of healthcare cybersecurity risks.

Key Findings from the Survey Include:

- 61% of institutions reported lacking formal, organization-wide cybersecurity audits that extend beyond technical assessments.

- Of those that conducted cybersecurity audits:

  - Only 43% incorporated evaluations of organizational behavior, governance structures, and cultural factors.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

- 57% relied solely on technical configurations and system-based controls.

- 72% indicated insufficient mechanisms to control user access rights, particularly for contractors and administrative personnel.

- 68% reported inadequate enforcement of confidentiality protocols, with shared login credentials and weak encryption practices prevalent.

- 59% acknowledged poor documentation or lack of system change traceability, undermining forensic readiness.

- 65% highlighted fragmented communication between cybersecurity teams and executive leadership as a barrier to effective governance.

- Notably, 70% of respondents identified insider threats and routine policy violations as persistent but under-assessed risks.

These findings reveal significant organizational and governance-related vulnerabilities that are often overlooked by traditional, technically focused audit practices. Qualitative IS audits, through their emphasis on human behavior, organizational culture, and governance processes, provide a structured approach for uncovering these hidden gaps.

Subsequent to identifying these deficiencies, institutions reported initiating several targeted interventions, including:

- Strengthening role-based access controls and implementing multi-factor authentication protocols.

- Embedding cybersecurity awareness and accountability into staff training and performance management.

- Establishing Internal Control Units (ICUs) tasked with continuous oversight of cybersecurity policies and risk mitigation.

- Revising vendor agreements to include explicit security performance metrics, right-to-audit clauses, and incident response requirements.

These corrective actions underscore the value of qualitative audits as diagnostic tools that illuminate institutional blind spots, inform risk-based interventions, and support the development of a resilient, security-conscious organizational environment.

Integrating Continuous Control Monitoring

The gaps uncovered through qualitative audits and the anonymous survey highlight that episodic assessments alone are insufficient for managing dynamic cybersecurity risks in healthcare environments. Continuous Control Monitoring (CCM) has emerged as a critical extension of qualitative audit practices, ensuring real-time oversight of both technical systems and human-driven vulnerabilities.

Survey Insights on Current State of Continuous Monitoring:

- Only **31%** of institutions reported having comprehensive CCM mechanisms in place that extend beyond technical performance metrics.

- Among organizations with CCM programs:

- 48% monitored only system uptime, patch compliance, and network traffic, without integrating user behavior or governance indicators.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

- Just 19% had mechanisms to flag deviations from approved access protocols or detect patterns of insider threat behavior.

- **74%** acknowledged the absence of automated tools capable of translating qualitative audit findings—such as weak security culture or policy non-compliance—into continuous, actionable metrics.

These statistics reinforce the need for healthcare institutions to evolve their approach to continuous monitoring, ensuring alignment with both technical and organizational risk factors.

Best Practices for Effective Continuous Control Monitoring:

Building on qualitative audit findings, healthcare institutions are increasingly adopting CCM frameworks that incorporate:

- Behavioral Risk Indicators: Continuous monitoring of abnormal user activities, such as excessive after-hours system access, irregular privilege escalations, and frequent policy deviations.

- Real-Time Policy Compliance Tracking: Automated alerts for lapses in critical controls, including outdated encryption, weak authentication, or deviations from established access management protocols.

- Governance Integration: Ensuring CCM outputs are reported not only to IT teams but also to executive leadership, internal control units, and governance committees for timely risk mitigation.

- Integration with Qualitative Audit Cycles: Using CCM data to inform subsequent audit activities, track the effectiveness of implemented controls, and provide early warnings of emerging vulnerabilities.

Case Application:

One healthcare system participating in the survey implemented a risk scoring mechanism following its qualitative audit. The system tracks:

- Access anomalies, including login attempts from unrecognized devices or locations.

- Policy violations, such as the use of shared credentials or unapproved software.

- Training compliance rates, ensuring staff complete mandatory cybersecurity education.

Since adopting this CCM approach, the institution has reported:

- A 46% reduction in unauthorized system access incidents.

- Faster detection and remediation of policy breaches.

- Improved executive visibility into organizational cybersecurity risks.

These outcomes demonstrate that when integrated effectively, continuous monitoring extends the impact of qualitative audits, creating an adaptive, intelligence-driven defense posture for healthcare institutions.

Lessons Learned from Health Institutions

The integration of qualitative information systems (IS) audits across healthcare institutions has revealed not only systemic cybersecurity vulnerabilities but also critical organizational lessons that can inform more resilient governance and risk management practices.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

Key Lessons Derived from Survey Data and Institutional Case Interventions:

Over-Reliance on Technical Controls Creates Blind Spots

The survey revealed that **57%** of institutions still rely predominantly on technical configurations and system-based assessments, neglecting critical human, behavioral, and governance dimensions of cybersecurity. Institutions that supplemented technical audits with qualitative assessments reported uncovering hidden risks—such as unsafe workarounds, cultural resistance to security protocols, and informal policy violations—that would have otherwise remained undetected.

Insider Threats Are Undervalued and Under-Monitored

Although **70%** of surveyed institutions identified insider threats as a persistent concern, fewer than **20%** had structured mechanisms in place to continuously monitor user behavior or evaluate the human factors contributing to insider risk. Qualitative audits brought much-needed visibility to this issue, prompting institutions to adopt insider threat matrices, behavior-based monitoring, and targeted awareness programs.

Fragmented Communication Undermines Risk Governance

A significant **65%** of institutions cited poor communication between cybersecurity teams and executive leadership as a barrier to implementing audit recommendations and ensuring cohesive risk management. Case studies demonstrated that embedding audit outputs into executive dashboards, governance committee agendas, and institutional performance metrics led to increased leadership engagement and accountability.

Cultural Factors Significantly Influence Cybersecurity Posture

Institutions that assessed organizational culture as part of their qualitative audits identified stark differences in security maturity between departments. For example, administrative units demonstrated weaker adherence to security protocols compared to clinical or IT teams. This insight allowed targeted interventions, including role-specific training and reinforced accountability structures.

Audit-Informed Training Drives Measurable Improvement

Qualitative audits that evaluated the effectiveness of awareness programs revealed substantial gaps between policy knowledge and real-world behavior. Institutions that redesigned their training programs based on audit findings—focusing on practical scenarios, behavioral expectations, and role-based risks—reported tangible improvements. One institution observed a **38%** decline in phishing susceptibility following audit-informed training enhancements.

Continuous Improvement is Essential, Not Optional

Healthcare organizations that treated qualitative audits as one-off exercises reported limited long-term impact. In contrast, those that integrated audits into ongoing risk management cycles, with periodic reassessments and continuous monitoring, experienced sustained improvements in security posture, policy compliance, and incident response readiness.

In conclusion, these lessons demonstrate that the true value of qualitative IS audits lies not only in identifying gaps but in catalyzing organizational learning, cultural change, and sustained governance reforms. Institutions that adopt a holistic, behaviorally informed, and continuously evolving approach to cybersecurity auditing are better positioned to withstand the evolving threat landscape and protect patient data, operational integrity, and institutional trust.

Vendor Risk and Third-Party Governance

The increasing reliance of healthcare institutions on third-party vendors, cloud services, and outsourced IT operations has significantly expanded the cybersecurity threat surface. While these partnerships offer

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

scalability and operational efficiency, they also introduce substantial risks related to data security, visibility gaps, and fragmented accountability.

Findings from the anonymous survey underscore the magnitude of these concerns:

- 74% of institutions reported inadequate oversight mechanisms for third-party vendors handling sensitive systems or data.
- Only 35% of vendor contracts included explicit cybersecurity requirements such as encryption standards, right-to-audit clauses, or breach notification obligations.
- 62% of respondents admitted to having limited visibility into the security practices of cloud providers or outsourced IT partners.
- Alarmingly, 48% of organizations had experienced at least one vendor-related security incident in the past 24 months, with many incidents traced back to insufficient due diligence or lack of contractual enforcement mechanisms.

These vulnerabilities were further validated through qualitative IS audits, which revealed common deficiencies, including:

- Absence of standardized risk-based vendor selection criteria.
- Over-reliance on verbal assurances rather than documented service-level agreements (SLAs).
- Lack of periodic, independent assessments of vendor security controls.
- Inconsistent application of shared responsibility models for cloud-based services.

Corrective Actions Informed by Audit Findings and Best Practices Include:

Formalized Vendor Governance Frameworks:

Healthcare institutions have begun establishing structured vendor management programs, requiring all third-party engagements to undergo security risk assessments prior to onboarding. These programs integrate cross-functional oversight from procurement, legal, IT, and cybersecurity teams to ensure comprehensive due diligence.

Contractual Security Provisions:

Revised vendor agreements now explicitly mandate technical and procedural safeguards, including:

- Data encryption requirements (at rest and in transit).
- Multi-factor authentication for vendor access to institutional systems.
- Right-to-audit clauses allowing independent verification of security controls.
- Defined breach notification timelines and financial penalties for non-compliance.

Continuous Vendor Performance Monitoring:

Institutions are leveraging automated tools and compliance scorecards to track vendor performance against contractual obligations. Metrics such as patching timelines, incident response readiness, and adherence to regulatory frameworks (e.g., HIPAA, HITECH) are continuously monitored and reviewed.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

Cloud Security Enhancements:

Recognizing the complexities of cloud environments, healthcare organizations have adopted shared responsibility models that clearly delineate security obligations between the institution and the cloud provider. Specific focus areas include:

- Data classification and secure storage practices.
- Identity and access management (IAM) protocols.
- Secure API integrations and encryption key management.
- Regular security assessments of Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) providers.

Third-Party Risk Committees and Oversight Boards:

To maintain strategic alignment and institutional accountability, organizations have established Cloud Risk Oversight Committees or Vendor Governance Boards. These bodies review vendor risk profiles, audit outcomes, and emerging third-party threats, ensuring that outsourced operations remain aligned with organizational cybersecurity policies.

In general, qualitative IS audits, coupled with systematic vendor governance reforms, have proven critical in mitigating the complex risks introduced by third-party relationships. By institutionalizing robust oversight mechanisms, contractual safeguards, and continuous monitoring, healthcare organizations can leverage external partnerships without compromising the confidentiality, integrity, or availability of sensitive health information.

Challenges and Limitations in Auditing Cybersecurity Programs

While qualitative information systems audits offer valuable insights for strengthening cybersecurity in healthcare, their effective implementation is often constrained by several challenges (Argaw et al., 2020). These limitations both institutional and methodological can reduce the accuracy, scope, or acceptance of audit findings.

Organizational Constraints

Healthcare institutions frequently operate with limited cybersecurity staffing, low audit budgets, and competing operational priorities. This creates several difficulties:

- Limited access to qualified cybersecurity personnel impedes the collection of in-depth audit data and restricts collaboration during the evaluation process.
- High turnover among IT and compliance staff disrupts audit continuity and institutional knowledge retention.
- Audit fatigue among stakeholders especially in high-demand clinical settings can result in superficial engagement with audit activities or resistance to follow-up actions.

Moreover, some institutions lack clearly defined governance frameworks, making it difficult to assign accountability for audit implementation and oversight.

Methodological Challenges

Conducting a robust qualitative audit requires skilled auditors with interdisciplinary expertise in IT, cybersecurity, risk management, and behavioral science. However:

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

- Inconsistent data availability limits the ability to triangulate findings from interviews, documents, and system observations.

- Language barriers or misalignment of technical terms between auditors and cybersecurity personnel can lead to misinterpretations of audit intent or findings.

- Bias in interview-based data collection may result in overstated control effectiveness or underreporting of known issues due to fear of reprisal or reputational concerns.

In some scenarios, qualitative approaches are undervalued compared to quantitative methods, reducing institutional support for in-depth, context-driven analysis.

Technical and Cultural Barriers

Healthcare organizations often rely on legacy systems and disconnected platforms, which limit visibility into enterprise-wide controls. Additional concerns include:

- Lack of standardized processes for capturing non-technical risks, such as social engineering exposure, insider threats, or informal workarounds.

- Cultural resistance to exposing systemic weaknesses, particularly in hierarchical environments where cybersecurity accountability is fragmented or broken.

- Cost sensitivity, especially in publicly funded or under-resourced institutions, may deprioritize investment in audit technology, continuous monitoring tools, or post-audit remediation.

Collectively, these challenges highlight the importance of designing qualitative audits that are tailored, resource-sensitive, and strategically aligned with institutional priorities. Solutions may include hybrid audit models, audit training for cross-functional teams, and incremental implementation strategies that build trust and demonstrate value over time.

Future Directions in Cybersecurity Auditing for Health Institutions

As healthcare systems continue to digitize and interconnect, cybersecurity auditing must evolve to address increasingly complex risks (Barnes & Daim, 2022). The limitations of traditional audit methods combined with the dynamic nature of cyber threats necessitate new frameworks, technologies, and collaborative approaches that support ongoing risk intelligence, not just retrospective compliance.

Advancing Qualitative IS Audit Techniques

Future auditing models will benefit from combining traditional qualitative methods with advanced analytical techniques that can capture subtle risk signals across large, complex systems. This includes:

- Implementing integrated control frameworks and fault-tree analysis to evaluate how governance structures, user behaviors, and system vulnerabilities interact.

- Creating healthcare-specific audit templates that enable efficient, repeatable assessments of clinical, administrative, and IT risk areas.

- Re-specifying traditional quantitative audit tools by incorporating qualitative variables such as staff behavior, policy comprehension, and role-based risk exposure.

These enhancements will allow auditors to detect early warning signs of cyber risk and evaluate security maturity more holistically.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

Integrating Artificial Intelligence and Machine Learning

AI has the potential to significantly enhance the scope, precision, and responsiveness of qualitative audits. By embedding intelligent agent models in the audit process, future audits could:

- Continuously learn from institutional behavior, policy violations, and control failures.
- Classify risks dynamically, adapting audit focus based on historical trends or live system input.
- Simulate audit outcomes across different business scenarios to support strategic planning and budgeting.

These tools can help shift cybersecurity auditing from static snapshots to dynamic, continuous assurance processes.

Public-Private and Cross-Sector Collaboration

To address systemic cybersecurity threats, future audit strategies must extend beyond individual institutions. Collaboration with:

- Public audit firms can provide independent oversight, policy benchmarking, and cross-institutional threat intelligence.
- Technology vendors and cloud providers allows for integrated audits of third-party risk exposure, especially as healthcare data infrastructure becomes more decentralized.
- Academic institutions can contribute empirical research, pilot studies, and training programs to advance qualitative IS auditing as a formal discipline.

A standardized cybersecurity audit classification framework developed in partnership with regulatory agencies could also support comparative evaluations and regulatory reporting.

Building a Resilient Cybersecurity Audit Ecosystem

Looking ahead, healthcare institutions should invest in audit ecosystems that are:

- Adaptable, so they can quickly respond to emerging threats, new technologies, and organizational shifts.
- Scalable, ensuring they work just as well in large integrated delivery networks as in smaller rural health systems.
- Inclusive, engaging not only IT and audit teams but also clinicians, HR, legal, procurement, and executive leadership.
- Ethical, by safeguarding privacy, reducing audit fatigue, and building trust among all stakeholders.

By embodying these principles, such ecosystems will strengthen cybersecurity defenses while promoting transparency, accountability, and a culture of continuous learning across the sector.

CONCLUSION AND RECOMMENDATIONS

With 82% of the U.S. population's health records compromised in 2024 alone, the current trajectory of healthcare data breaches reveals a dire need for rethinking existing cybersecurity governance (HIPAA Journal, 2024). The growing scale and complexity of cyber threats facing U.S. healthcare institutions demand a more comprehensive and human-centered approach to cybersecurity oversight (Jalali & Kaiser, 2018). While traditional audit frameworks remain valuable, they often fall short in identifying the deeply rooted behavioral,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VII July 2025

cultural, and governance-related vulnerabilities that drive many of today's most severe breaches (Jalali & Kaiser, 2018).

This study has demonstrated that qualitative information systems audits offer a vital tool for uncovering these deeper organizational issues, enabling auditors to assess not just the presence of technical controls but the context in which they operate. By applying a novel framework grounded in Intelligent Agent modelling, the proposed audit approach enhances insight generation, facilitates dynamic risk classification, and provides healthcare leaders with more actionable and impactful audit outcomes. Qualitative audits empower institutions to move beyond superficial checkbox compliance and toward strategic, data-driven cybersecurity governance. When embedded within enterprise risk management systems, these audits foster greater accountability, stakeholder awareness, and a culture of continuous improvement, essential attributes for building resilient and secure health organizations(Martin, 2020).

Key Findings and Implications

- Healthcare institutions continue to face disproportionate cybersecurity risks, driven by system complexity, workforce behavior, and fragmented controls.
- Traditional, metrics-based audits inadequately address these risks due to their limited scope and abstraction from human and organizational factors.
- Qualitative IS audits provide richer, contextual insight by evaluating user behavior, policy implementation, governance structure, and institutional culture.
- The proposed IA-enhanced qualitative audit model improves audit adaptability, precision, and responsiveness in dynamic health environments.
- Institutions that integrate audit outcomes into strategic planning experience improvements in control maturity, compliance posture, and organizational resilience.

Strategic Recommendations for Practice

To operationalize the insights gained from this study, we propose the following recommendations:

Establish Internal Control Units in Hospitals.

Hospitals should create internal control and audit units staffed with cybersecurity and compliance professionals to monitor policy adherence, assess behavioral risks, coordinate across departments, and oversee third-party access and change management.

Adopt Hybrid Audit Frameworks.

Combining qualitative and quantitative methods ensures both technical configurations and organizational practices are effectively evaluated, offering a more comprehensive view of cybersecurity risks.

Embed Audit Feedback into Institutional Strategy.

Audit results should inform key decisions in budgeting, procurement, clinical governance, and digital transformation, aligning cybersecurity insights with long-term strategic planning.

Invest in Audit Technology and Automation.

AI-enabled tools, including intelligent agent models, should be used to simulate risks, automate findings classification, and support continuous monitoring of controls and behavior.

Foster a Culture of Shared Cybersecurity Responsibility.

All personnel should be trained on cybersecurity expectations, with workflows and protocols designed to embed accountability and security-conscious behavior throughout the organization.

Build Cross-Functional Audit Teams.

Audits should involve interdisciplinary teams across IT, compliance, legal, privacy, and clinical areas to ensure balanced assessments and promote implementation buy-in.

Develop Sector-Wide Standards for Qualitative Cyber Auditing.

Regulatory bodies and associations should establish standardized tools and benchmarks to guide qualitative audits, support compliance, and enable cross-institutional comparisons.

REFERENCE

1. Afifi, M. A. M. (2020). Assessing information security vulnerabilities and threats to implementing security mechanism and security policy audit. Journal of Computer Science, 16(3), 321–329. https://doi.org/10.3844/jcssp.2020.321.329
2. Argaw, S., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20, Article 61. https://doi.org/10.1186/s12911-020-01161-7
3. Barnes, B., & Daim, T. (2022). Information security maturity model for healthcare organizations in the United States. IEEE Transactions on Engineering Management, 71, 1–12. https://doi.org/10.1109/TEM.2021.3139836
4. Cartwright, A. J. (2023). The elephant in the room: Cybersecurity in healthcare. Journal of Clinical Monitoring and Computing, 37(5), 1123–1132. https://doi.org/10.1007/s10877-023-01013-5
5. Data Breaches: Why personal information is so valuable to cybercriminals. (2021). Milwaukee Independent. Retrieved from https://www.milwaukeeindependent.com/syndicated/data-breaches-personal-information-valuable-cybercriminals/
6. Giansanti, D. (2021). Cybersecurity and the digital health: The challenge of this millennium. Healthcare, 9(1), Article 62. https://doi.org/10.3390/healthcare9010062
7. HIPAA Journal. (2025, January 30). 2024 healthcare data breach report. HIPAA Journal. Retrieved from https://www.hipaajournal.com/2024-healthcare-data-breach-report/
8. Ilıkhan, S. U., Özer, M., Tanberkan, H., & Bozkurt, V. (2024). How to mitigate the risks of deployment of artificial intelligence in medicine? Turkish Journal of Medical Sciences, 54(3), 483–492. https://doi.org/10.55730/1300-0144.5814
9. Jalali, M. S., & Kaiser, J. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059
10. Kahyaoğlu, S. B., & Çalıyurt, K. T. (2018). Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal, 33(4), 360–376. https://doi.org/10.1108/MAJ-02-2018-1804
11. Kegerreis, M., Schiller, M., & Davis, C. (2020). IT auditing: Using controls to protect information assets (3rd ed.). McGraw-Hill Education.
12. Martin, N. (2020). Enabling effective oversight: Enterprise risk management and board governance in healthcare. Healthcare Management Forum, 33(4), 182–191. https://doi.org/10.1177/0840470420907260
13. Matas, S. D., & Keegan, B. J. (2020). Challenges in addressing information security compliance in healthcare research: The human factor. American Journal of Operations Management and Information Systems, 5(2), 25–40. https://doi.org/10.11648/j.ajomis.20200502.12
14. Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy, 3(3), 327–345. https://doi.org/10.3390/jcp3030017
15. Naik, N., Hameed, B. M. Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Prasad, B., Chłosta, P., & Somani, B. (2022). Legal and ethical consideration in artificial intelligence in healthcare: Who takes responsibility? Frontiers in Surgery, 9, Article 862322. https://doi.org/10.3389/fsurg.2022.862322

16. Park, W., Seo, S.-W., Son, S.-S., Lee, M., Kim, S.-H., Choi, E., Bang, J.-E., Kim, Y.-E., & Kim, O.-N. (2010). Analysis of information security management systems at five domestic hospitals with more than 500 beds. Healthcare Informatics Research, 16(2), 89–99. https://doi.org/10.4258/hir.2010.16.2.89
17. Ronquillo, J. G., Winterholler, J., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information. JAMIA Open, 1(1), 15–19. https://doi.org/10.1093/jamiaopen/ooy019
18. Schiliro, F. (2023). Building a resilient cybersecurity posture: A framework for leveraging prevent, detect and respond functions and law enforcement collaboration [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2303.10874
19. Sow, M., & Gehrke, C. (2019). Evaluating information security system effectiveness for risk management, control, and corporate governance. Business and Economic Research, 9(1), 164–174. https://doi.org/10.5296/ber.v9i1.13994
20. Stafford, T. F., Deitz, G. D., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal, 33(4), 410–424. https://doi.org/10.1108/MAJ-07-2017-1596
21. Vukotich, G. (2023). Healthcare and cybersecurity: Taking a zero trust approach. Health Services Insights, 16, Article 11786329231187826. https://doi.org/10.1177/11786329231187826
22. Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18(2), 101–113. https://doi.org/10.1057/ejis.2009.12
23. Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in Digital Health, 4, Article 862221. https://doi.org/10.3389/fdgth.2022.862221