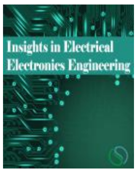
Lanash
Insights in Electrical Electronics Engineering
Research Paper
Volume 2 Issue 1
Published 19 August 2025



Integrating Technology Risks, Compliance, Audits, and Privacy

C.A. Alexander*[1] and L. Wang[2]

[1]Institute for IT Innovation and Smart Health, Mississippi, USA
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA

Submitted on 06 June 2025
Accepted on 11 July 2025
Published on 19 August 2025

To cite this article: C.A. Alexander and L. Wang, "Integrating Technology Risks, Compliance, Audits, and Privacy," *Insight. Electr. Electron. Eng.*, vol. 2, no. 1, pp. 1-6, 2025.

Abstract

Technologies such as the cloud, information and communications technology (ICT), the Internet of Things (IoT), and wearable wireless medical sensor networks have brought benefits and opportunities; however, they have also introduced increased risks and challenges. This paper introduces technology risks, compliance, audits, and privacy. ICT-based assets, cloud, IoT, wearable wireless medical sensor networks, etc., often suffer from cyberattacks. A compliance audit is often needed. Privacy and security issues can arise in various areas, including devices, storage, and communication. This paper will also present a case study of integrating technology risks, compliance, audits, and privacy in the Emerald Healthcare System. Advanced technologies, adherence to compliance, regular auditing, privacy protection, and related controls for vulnerabilities and cyber risks help Emerald Healthcare System practice robust cybersecurity.

Keywords: cybersecurity; cyber risks; technology risks; compliance; audits; privacy; blockchain; Internet of Things; Internet of Medical Things; healthcare

Abbreviations: ICT: information and communications technology; IoT: Internet of Things; DL: deep learning; BI: business intelligence; FMEA: failure mode and effects analysis; FAIR: factor analysis of information risk; IoMT: Internet of Medical Things; ECC: essential cybersecurity controls; RC2AS: risk-based cybersecurity compliance assessment system; PP-ADV: privacy-preserving authentication with device verification

1. Introduction

Technologies such as the cloud, information and communications technology (ICT), Internet of Things (IoT), big data analytics, and deep learning (DL) bring up opportunities, benefits, increased risk, and challenges. Auditing, especially real-time auditing, needs a data-driven approach or data analytics. An organization needs regular auditing and follows standards or regulations for compliance due to increasing cyber risks. A compliance audit is often needed, requiring the submission of internal control documents to a neutral auditor outside. Security and privacy are different. Security is the protection against unauthorized access to data or valuable information. Privacy is regarding user-specific details found in data that must be kept secure [1, 2].

There is a team for collecting large data to view and make decisions about security in most companies with a cybersecurity team. Besides many tools of business intelligence (BI) and analytics that connect to where the data is stored, there are tools and software for collecting and managing data in databases and data lakes. There should be contractual requirements for the third party. Clear contract language is used for managing third-party risks and cybersecurity. It is necessary to have a private addendum or privacy language in the base contract to meet privacy regulations if customers' private data is shared with a vendor. Secure software development is the process that puts security directly into the development of software or hardware during its lifecycle. This process needs to be documented and validated as being followed and internally tested. An on-site assessment is the validation standard of vendor security controls. Scheduling, investigation, assessment, reporting, and remediation (if required) are the five phases of an on-site assessment. Much of the on-site assessment can be conducted virtually if tools are available [2].

Risk analysis is dynamic. It should be regular due to changing situations. Valuable risk analysis is actionable, realistic, and reproducible. Failure mode and effects analysis (FMEA) is a risk analysis method regarding the failure mode and the effects of failures. Business impact analysis is used to find the necessary functions of an enterprise and analyze the impacts of an interruption. Factor analysis of information risk (FAIR) is useful for qualitative and quantitative analysis. A common method of third-party analysis is skipping the risk analysis and jumping into a gap analysis against the controls that should be in place [1].

The primary purpose of the research in this paper is to deal with the integration of technology risks, compliance, audits, and privacy. The remainder of this paper will be organized as follows: the second section introduces technology risks (such as cyber risks due to the adoption of the cloud, IoT/IoMT, wearable wireless medical sensor networks, etc.); the third section presents compliance; the fourth section introduces audits; the fifth section presents privacy and security; the sixth section is a case study of integrating technology risks, compliance, audits, and privacy; and the seventh section is the conclusion.

*Corresponding Author:
C.A. Alexander, Institute for IT Innovation and Smart Health, Mississippi, USA

2. Technology Risks

ICT enables a hospital to provide richer services at a higher level of quality; however, it also expands the cyberattack surface. A smart hospital has many ICT-based assets, as shown in **Figure 1** [3]. Every asset has a cyberattack surface, leading to the exposure of the ICT-supported hospital to various cyberattacks.

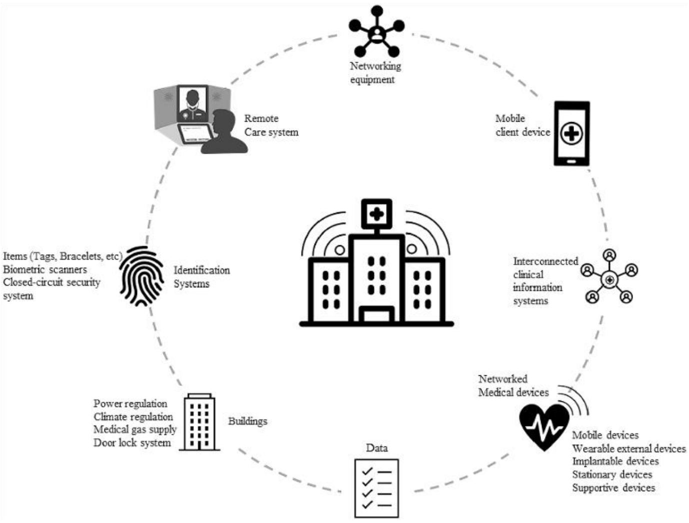


FIGURE 1: An ICT-based smart hospital.

The IoT has been widely used; however, it also causes cyber risks or cyberattacks. Blockchain helps prevent cyberattacks and enhance cybersecurity. **Figure 2** illustrates blockchain and machine learning on the Internet of Medical Things (IoMT). Machine learning is powerful in data analytics and prediction. The cloud server is used for data processing and storage; it is directly connected to the healthcare application layer.

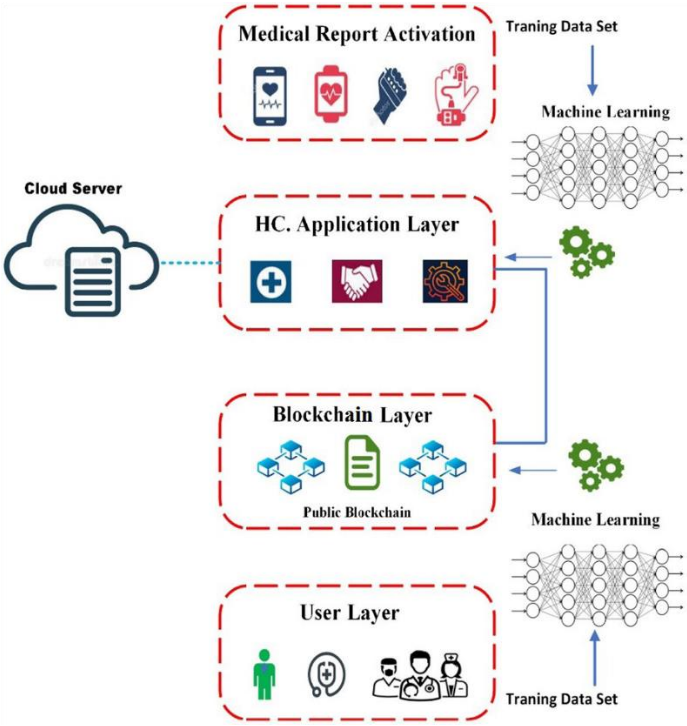


FIGURE 2: Blockchain and machine learning on the IoMT.

A wireless medical sensor network has been presented, as shown in **Figure 3** [4]. It comprises the following parts: wearable medical sensor nodes (WeMSN), zonal nodes (ZN), central medical server (CMS), local medical server (LMS), and medical/clinical experts. WeMSN is implanted in patients' bodies to capture data such as blood pressure and blood glucose levels through the ZN. ZN (also sensor nodes) aggregate patients' data from WeMSN. CMS performs massive storage and computation. Besides performing computation, processing, and storage, LMS implements signature verification during text data transmission and implements verification after signatures are gathered through the ZN. Medical/clinical experts review data through CMS and LMS, perform diagnoses, and make decisions on treatment and medication. Medical data transmission is tremendously vulnerable to cyberattacks; therefore, signatures and verifications are performed to mitigate cyber risks [4].

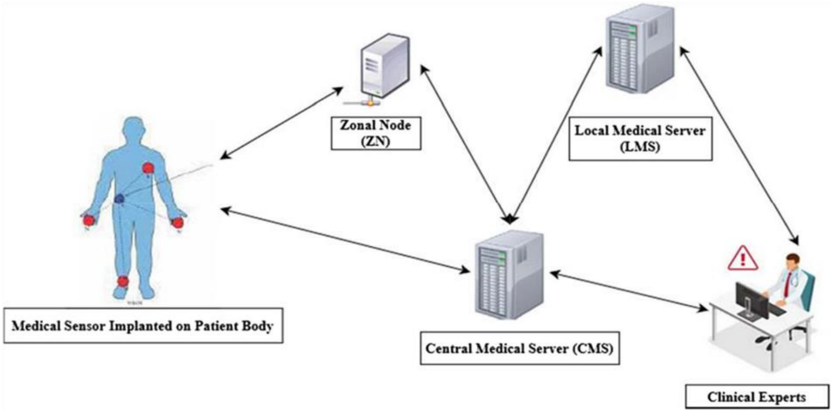

Zonal Node (ZN)
Local Medical Server (LMS)
Medical Sensor Implanted on Patient Body
Central Medical Server (CMS)
Clinical Experts

FIGURE 3: Wearable wireless medical sensor network.

3. Compliance

Essential cybersecurity controls (ECC) were taken as a baseline to develop a risk-based cybersecurity compliance assessment system (RC2AS). Various compliance-calculation methods have been compared according to their purposes and uses, which is shown in **Table 1** [5]. The method 'RC2AS weighted compliance' enables a reasonable and correct evaluation, measuring the present level of cybersecurity compliance with the ECC.

TABLE 1: Comparison of various compliance-calculation methods.

Methods	Purposes and uses
Strict compliance	It helps to completely abide by the control & requirements. A weak hole within the control causes the entity's exposure and prevents the realization of control objectives.
Semi-strict compliance	It counts the efforts that have been made to meet requirements by raising the compliance score of the requirements of control.
Weighted compliance	It distinguishes implementation levels & offers a more specific score on implemented requirements.
RC2AS weighted compliance	It has a better understanding of the domain & status of an enterprise by distinguishing enterprises with various scopes, business functionalities, & criticality levels. It also includes the risk levels of subdomains.

A conceptual model was developed based on hypotheses to check the influence of an individual's decision-making style on the cybersecurity compliance behavior of an employee, as shown in **Figure 4** [6]. The cybersecurity compliance behavior is hypothesized as follows: 1) be positively affected by the employee's perceived or observed severity (H1), 2) be positively affected by the observed vulnerability (H2), 3) be positively affected by the self-efficacy (H3), 4) be positively affected by the response efficacy (H4), 5) be negatively affected by the observed barriers (H5), and 6) be positively affected by the security awareness (H6) [6].

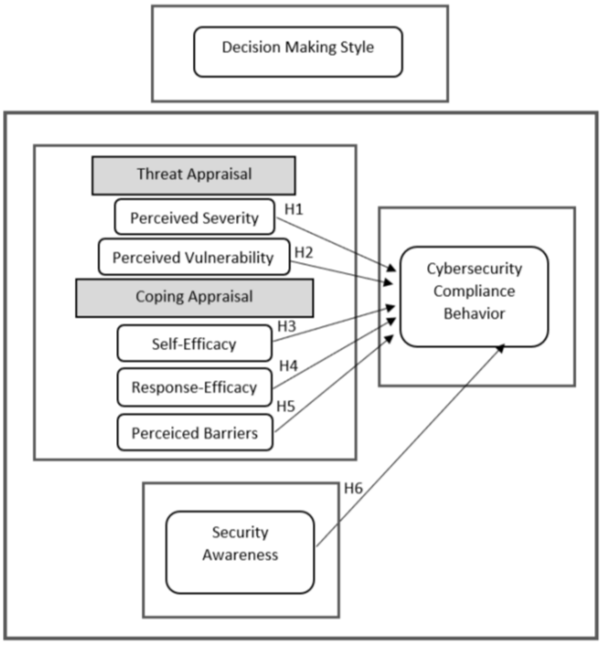


FIGURE 4: A conceptual model regarding cybersecurity compliance behavior.

4. Audits

An audit is known as a practice for safety assurance and quality. An audit platform with three layers (database, server, and client) was developed. There are data grids, an audit calendar, and the function of professional authentication on the audit platform [7]. The effectiveness of the internal audit of cybersecurity was analyzed. A Cybersecurity Audit Index was used, which consists of three dimensions (planning, performing, and reporting). It is demonstrated that the index is positively related to cyber risk management maturity, but it is not associated with the probability of a successful cyberattack [8].

Internal auditors face many expectations regarding data privacy, cybersecurity, and technologies. They should promote new skills regarding information technology and systems [9]. The HIPAA Audit Program reviews policies and procedures. A HIPAA security and privacy compliance audit and risk assessment mitigation can be achieved by creating a network [10].

5. Privacy and Security

Privacy issues in IoT include device privacy, storage privacy, and communication privacy. Reliability should be considered for personal devices. Algorithm encryption can be used to protect storage privacy. Secure protocols should be employed in communication [11]. Privacy-preserving authentication with device verification (PP-ADV) was presented to secure a healthcare system on a 5G network. Many IoT devices were used to collect patients' sensitive information, which was processed and stored in the computing system. A self-compiling system with registration and authentication functions was developed to provide secure diagnosis and treatment in a digital healthcare system, as illustrated in **Figure 5** [12].

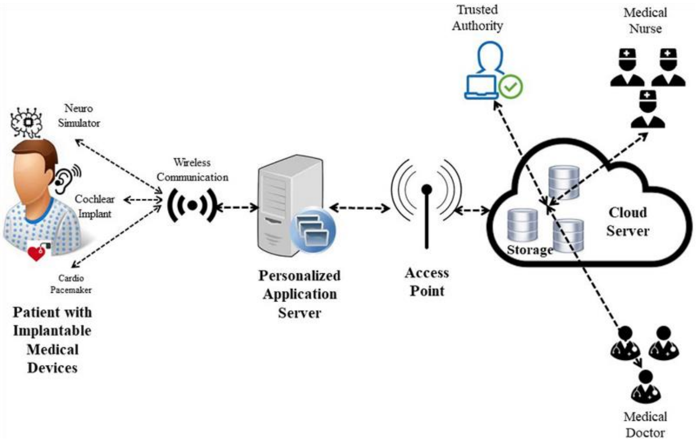


FIGURE 5: A digital healthcare system based on PP-ADV.

A method of privacy assessment was presented that covers six aspects, which are shown in **Table 2** [13]. Among the aspects, disclosure of information is a major focus. Vulnerabilities or threats should be analyzed carefully to choose suitable controls. During the analysis process, the vulnerability types, description, and data flow interactions should be considered to enhance security and protect privacy. **Table 3** [14] lists controls for mitigating various vulnerabilities.

TABLE 2: Aspects related to privacy assessment.

Threats	Security violated	Description of threats
Information disclosure	Confidentiality	Information access without authorization
Privilege elevation	Authorization	Permitting unauthorized access
Denial of service (DoS)	Availability	Flooding a targeted machine or resources with requests and making the machine or resources unavailable to intended users.
Tampering	Integrity	Data, software, or network modification, fabrication.
Spoofing	Authentication	Identity pretense, masquerading, e.g., Sybil attack
Repudiation	Non-repudiation	Denial of action, honest but curious behaviors

TABLE 3: Controls for various vulnerabilities.

Vulnerabilities	Controls
Lack of validation in data input	Input validation, data integrity
Weak schemes of authentication	Authentication
Lack of encryption on data transmission	Communication security, encryption
Weak control of remote access	Access control
Lack of encryption on sensitive or private data at rest	Encryption
Weak credentials transit	Encryption, authentication
Lack of physical tamper detection & responses	Physical protection
Lack of system hardening	Client platform security, physical protection
Possible data repudiation due to Android or iOS applications	Non-repudiation, auditing

6. A Case Study

Emerald Healthcare System is a not-for-profit corporation dedicated to developing medical programs, healthcare services, research, etc. The system's three hospital campuses, plus several outpatient facilities, offer a broad spectrum of care. Services provided by over 1,550 medical staff members and more than 10,300 employed professionals make Emerald Healthcare System one of the largest healthcare providers in Texas, USA.

6.1. Technology risks and diverse pressures due to risks

Technology is exploding in healthcare systems such as the Emerald Healthcare System and has multiple advantages, such as how easily data is generated, stored, and transferred between systems and facilities. This proliferation in data works well and allows for improved healthcare management from diagnosis to treatment and better patient care. Cloud computing powers many of these data capabilities and fosters the potential risk for data access by malicious third parties, especially for cloud-connected medical devices and related software. Without the appropriate security protocols, connected medical devices may be altered and accessed to change functionality.

Major stakeholders in the Emerald Healthcare System include patients, employers, physicians, pharmacists, etc. It must create a robust cybersecurity program for all stakeholders; however, it has a shortage of professionals and resources in cybersecurity. Staff members and employees have a weak awareness of cyber risks, and management tends to function with low levels of effective management. These problems contribute to the pressures of creating a comprehensive risk management approach.

6.2. Compliance and audits

Compliance for Emerald Healthcare System must include HIPAA and other government standards and ethics compliance. Risk and compliance leaders must sustain constant pressure to do more with less as they are tasked to meet regulatory requirements and address an expanded risk agenda while managing costs and increasing efficiency. Compliance and risk management leaders face increased pressure to be more agile in mitigating evolving risks and enhancing compliance from regulators, internal stakeholders, and examiners. Tech-driven and data-rich, they must deliver sound, cost-effective risk and compliance programs. Using extensive audit processes can reduce pressure on managers. Audits are also posited to increase accountability and improve the quality of healthcare at a facility using systematic monitoring and evaluation.

Several types of audits are used to improve healthcare. They include external audits, used to gain insight into a hospital's compliance with external criteria (e.g., accreditation, certification, external peer review, etc.); clinical audits, which are performed as a local initiative by healthcare professionals; and internal audits, which are most often used in preparation for an external audit.

6.3. Privacy and security

In the Emerald Healthcare System, protecting patients' privacy is at the core of the staff, providers, and all professionals. If a lack of privacy causes a leak in patient data, there could be serious consequences, including but not limited to fines, loss of business or job security, and jail. Patient data is more important and valuable than a Social Security card number or a credit card number. Malicious actors can sell patient data to third parties, which could prevent the patient from being insured, cause problems with finding a provider, etc. There are numerous ways to leak patient data in the hospital. This includes spoken words while on a break to a coworker or visitor, mining the patient record while on your own time, and any other reason a staff member should not be in a patient record.

Data privacy evolved from a regulatory compliance initiative to a customer trust imperative. Emerald Healthcare System can now map how the primary business value of data privacy programs mitigates risk by ensuring compliance. Mature programs become a strategic driver of business value and customer trust. Data breaches and cyberattacks are costly, but cyber liability insurance can help cover the cost of the healthcare system. These costs can include lost income due to a cyberattack, costs associated with notification of those affected by the breach, costs for recovering compromised data, costs related to damaged systems, and more.

7. Conclusion

ICT-based assets, cloud, IoT, such as IoMT, wearable wireless medical sensor networks, etc., often suffer from cyber-risks and cyberattacks. Medical data transmission is also tremendously vulnerable to cyberattacks. Blockchain helps prevent cyberattacks and enhance cybersecurity. An audit is known as a practice for safety assurance and quality. A compliance audit is often needed. Privacy issues can arise in various areas, including devices, storage, and communication. Advanced technologies, adherence to compliance (aspects of standards, regulations, technologies, etc.), regular auditing, privacy protection, and related controls for vulnerabilities and cyber risks help Emerald Healthcare System practice robust cybersecurity.

Ethics

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

Declaration of the use of AI tools

The authors declare that they did not use AI tools in writing this paper.

Conflicts of Interest

The authors would like to announce that there is no conflict of interest.

Acknowledgments

The authors would like to express thanks to Technology and Healthcare Solutions, USA, for its help and support.

References

[1] R. Pompon, IT Security Risk Control Management – An Audit Preparation Plan, Berkeley, CA: Apress, 2016.

[2] G. Rasner. (2021, June). *Cybersecurity and third-party risk* [Online].

[3] L. Coppolino, L. Sgaglione, S. D'Antonio, M. Magliulo, L. Romano, and R. Pacelli, "Risk assessment driven use of advanced SIEM technology for cyber protection of critical e-health processes," *SN Computer Science*, vol. 3, October 2022.

[4] O. B. J. Rabie, S. Selvarajan, T. Hasanin, G. B. Mohammed, A. M. Alshareef, and M. Uddin, "A full privacy-preserving distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless medical sensor networks (HWMSNs)," *International Journal of Information Security*, vol.23, no. 1, pp. 51-80, November 2023.

[5] A. Alfaadhel, I. Almomani, and M. Ahmed. "Risk-based cybersecurity compliance assessment system (RC2AS)," *Applied Sciences*, vol. 13, no. 10, pp. 6145, May 2023.

[6] A. Duzenci, H. Kitapci, and M. S. Gok, "The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior," *Applied Sciences*, vol. 13, no. 15, pp. 8731, July 2023.

[7] R. Sousa, C. Esteves, A. Abelha, and H. Peixoto, "Streamlining Healthcare Quality Management with an Web Audit Platform," *Procedia Computer Science*, vol.238, pp. 944-949, 2024.

[8] S. Slapničar, T. Vuko, M. Čular, and M. Drašček, "Effectiveness of cybersecurity audit," *International Journal of Accounting Information Systems*, vol. 44, pp. 100548, March 2022.

[9] L. R. Hepworth, C. Greenman, D. Esplin, and R. Johnston, "Cybersecurity and Data Privacy: The Rising Expectations Within Internal Audit," *Journal of Forensic and Investigative Accounting*, vol. 14, SI. 3, 2022.

[10] Y. B. Choi and C. E. Williams, "A HIPAA security and privacy compliance audit and risk assessment mitigation approach," in Research Anthology on Securing Medical Systems and Records, USA: IGI Global, pp. 706–725, 2022.

[11] A. Parihar, J. B. Prajapati, B. G. Prajapati, B. Trambadiya, A. Thakkar, and P. Engineer, "Role of IOT in healthcare: Applications, security & privacy concerns," *Intelligent Pharmacy*, vol 2, no. 5, pp. 707-714, October 2024.

[12] M. R. Patruni, and A. G. Humayun, "PPAM-mIoMT: a privacy-preserving authentication with device verification for securing healthcare systems in 5G networks," *International Journal of Information Security*, vol. 23, no. 1, pp. 679-698, October 2023.

[13] O. Popool, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehia, and J. Popoola, "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions," *Blockchain: Research and Applications*, vol. 5, no. 2, pp. 100178, June 2024.

[14] P. C. Paul, J. Loane, F. McCaffery, and G. Regan, "Towards design and development of a data security and privacy risk management framework for WBAN based healthcare applications," *Applied System Innovation*, vol. 4, no. 4, pp. 76, September 2021.