Grenze International Journal of Engineering and Technology, June Issue

A Comprehensive Survey of Information Security Compliance Frameworks

Sahana Shettigar[1] and Raju K[2]
[1-2]NMAM Institute of Technology, Nitte (Deemed to be University) Nitte /Department of Computer Science, India
Email: nnm24cys13@nmamit.in, rajuk@nitte.edu.in

***Abstract*—The rapid expansion of cloud computing and digital services has significantly increased the complexity of information security management in modern organizations. To address these challenges, several security compliance frameworks have been developed to guide organizations in protecting sensitive data and maintaining regulatory compliance. This paper provides a comparative survey of widely adopted frameworks, including ISO/IEC 27001, SOC 2, HIPAA, GDPR, and PCI DSS. The study examines their governance structures, control mechanisms, certification processes, and regulatory scopes. It also explores the operational challenges organizations face when implementing multiple compliance frame-works simultaneously. In addition, the paper discusses emerging approaches such as automation and artificial intelligence that support continuous compliance monitoring in cloud environments. The findings suggest that integrated compliance strategies can improve governance efficiency while strengthening cybersecurity resilience across complex digital infrastructures.**

I. INTRODUCTION

The widespread adoption of cloud computing has significantly influenced how organizations manage sensitive information. [5], [13]. Organizations now depend heavily on digital systems for daily opera-tions. Today's businesses, government agencies, and service providers operate increasingly complex digital infrastructures that extend across geographic and technological boundaries. These develop-ments provide substantial operational advantages but also introduce significant cybersecurity risks and regulatory challenges. Security and compliance requirements have therefore become significantly more demanding for modern organizations.

In response, the information security community has developed several frameworks to help organiza-tions safeguard information assets and maintain secure operational practices. ISO/IEC 27001 provides a systematic methodology for establishing Information Security Management Systems based on risk assessment and continuous improvement principles [1]. Complementary frameworks such as SOC 2 and regulatory requirements including HIPAA and GDPR also define standards for protecting sensitive organizational and personal data [3], [4], [8].

However, organizational reality rarely aligns with single-framework compliance scenarios. Many or-ganizations must satisfy multiple regulatory and industry requirements simultaneously. A cloud service provider, for example, may require SOC 2 attestation, implement ISO 27001 controls, and demonstrate GDPR compliance to meet customer and regulatory expectations [8], [3]. Similarly, organizations pro-cessing payment card information must adhere to PCI DSS security requirements alongside these other standards [2], [17].

As a result, managing compliance across multiple frameworks can become increasingly complex for organizations.

Grenze ID: 01.GIJET.12.2.342_24

Although these frameworks often share similar security objectives, they frequently dif-fer in terminology, control structures, and assessment approaches. Organizations must therefore coor-dinate their security practices carefully to avoid duplicated compliance efforts while maintaining com-prehensive regulatory coverage [14], [19]. This study presents a comparative analysis of major infor-mation security compliance frameworks and explores how automation and artificial intelligence can improve compliance management in cloud environments [12], [15].

II. Related Work

A growing body of research highlights the role of information security compliance frameworks in sup-porting governance, risk management, and regulatory accountability across cloud-based and distribut-ed systems [15], [19]. Frameworks such as ISO/IEC 27001 provide structured approaches for imple-menting Information Security Management Systems (ISMS) through risk assessment and continuous improvement, strengthening organizational security and resilience [1].

Regulatory frameworks such as GDPR and HIPAA enforce requirements for protecting sensitive per-sonal and healthcare data, emphasizing transparency, accountability, and data governance [3], [4]. Ser-vice-oriented frameworks such as SOC 2 demonstrate control effectiveness and build trust in cloud services, while PCI DSS defines technical requirements for securing payment card data [2], [8]. Togeth-er, these frameworks address complementary aspects of information security governance, often requir-ing integrated compliance strategies.

Recent studies highlight the role of automation and artificial intelligence in improving compliance management. Automated tools support continuous monitoring and evidence collection, while machine learning techniques detect anomalies and potential compliance violations, enabling more effective governance in dynamic environments [12], [17].

III. Methodology

This study adopts a comparative survey methodology to evaluate widely implemented information se-curity compliance frameworks in cloud computing environments. Five major frameworks—ISO/IEC 27001, SOC 2, HIPAA, GDPR, and PCI DSS—were selected based on their global adoption, regulatory relevance, and applicability to modern digital infrastructures [1], [2], [3], [4], [8].

For systematic comparison, the frameworks were analyzed across common security control domains, including access control, encryption, logging and monitoring, incident response, and third-party risk management. These domains enable identification of overlapping controls and differences in imple-mentation across frameworks [14], [17].

The methodology also references the compliance implementation lifecycle illustrated in Fig. 1, includ-ing control deployment, monitoring, validation, and continuous improvement, along with the role of automation and artificial intelligence in supporting continuous compliance monitoring [12], [15].

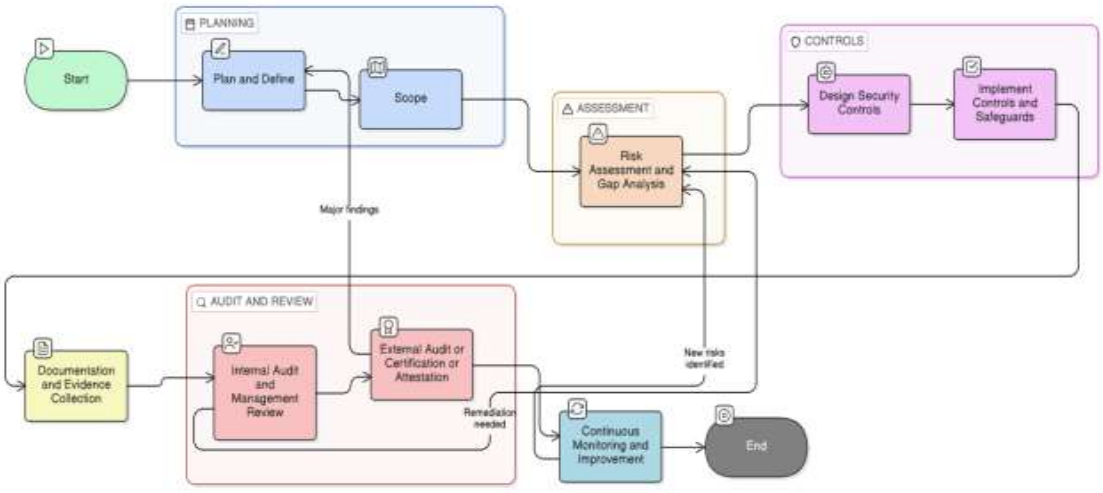

Fig. 1. Compliance Implementation and Validation Lifecycle Across Security Framework

IV. Overview of Major Information Security Compliance Frameworks

Information security compliance frameworks have evolved to address increasing governance require-ments in modern digital infrastructures and cloud computing environments where organizations man-age sensitive information across distributed systems. Several frameworks now guide organizations in implementing structured security management practices.

Among these frameworks, ISO/IEC 27001 is widely recognized as a comprehensive international stand-ard for establishing Information Security Management Systems within organizations [1]. The standard emphasizes risk-based security management and continuous improvement of security processes. Or-ganizations implementing ISO/IEC 27001 integrate security practices into governance structures and operational workflows. Certification requires organizations to undergo formal audits conducted by ac-credited external assessors. Successful certification demonstrates that organizational security controls align with internationally recognized information security management practices.

SOC 2 serves as an assurance framework designed primarily for technology and cloud service provid-ers. It evaluates internal controls based on the Trust Services Criteria, including security, availability, confidentiality, processing integrity, and privacy [8]. Organizations often obtain SOC 2 attestation to demonstrate reliability and operational security to enterprise customers. These reports provide inde-pendent verification that service providers maintain effective security controls within their operational environments.

Regulatory frameworks such as HIPAA and GDPR establish legally binding requirements for protecting healthcare information and personal data within digital systems [3], [4]. HIPAA defines administrative, technical, and physical safeguards to protect electronic protected health information. GDPR focuses on transparency, accountability, and protection of personal data belonging to individuals.

Another widely implemented framework is the Payment Card Industry Data Security Standard, which governs the protection of payment card information within financial transaction ecosystems [2]. Organ-izations processing payment card data must comply with specific technical and operational security controls. These requirements include encryption, access restrictions, and continuous monitoring of payment processing systems. Together, these frameworks form the foundation of modern information security governance across many industries.

A. Scope Comparison

The scope of information security compliance frameworks varies significantly in terms of industry fo-cus, regulatory enforcement, and governance objectives across different operational environments. Some frameworks function as voluntary standards adopted to strengthen organizational security gov-ernance. Others impose legally binding requirements designed to protect sensitive personal, healthcare, or financial information [3], [4].

ISO/IEC 27001 and SOC 2 primarily operate as voluntary governance and assurance mechanisms that organizations adopt to demonstrate security maturity and operational reliability to stakeholders [1], [8].In contrast, regulatory frameworks such as HIPAA and GDPR impose mandatory obligations for protecting healthcare information and personal data. Organizations that process payment card infor-mation must also comply with the PCI DSS framework, which defines technical security requirements for financial transaction environments [2]. These frameworks differ in scope but share common objec-tives related to protecting sensitive information assets.

TABLE I: HIGH-LEVEL COMPARISON OF INFORMATION SECURITY COMPLIANCE FRAMEWORKS

Parameter	ISO/IEC 27001	SOC 2	HIPAA	GDPR	PCI DSS
Type	International Standard	Audit / Attestation Framework	Government Regulation	Government Regulation	Industry Standard
Primary Objective	Establish and maintain Information Security Management System (ISMS)	Assure custom-ers about control effective-ness	Protect healthcare data (PHI/ePHI)	Protect person-al data and pri-vacy	Secure payment card data
Industry Focus	All industries	Cloud, SaaS, IT services	Healthcare sector	All industries	Payment card indus-try
Geographical Scope	Global (volun-tary)	Global (custom-er-driven)	United States	EU + global applicability	Global
Mandatory or Optional	Optional	Optional (market-driven)	Mandatory	Mandatory	Mandatory
Data Protected	Information assets	Customer data	Protected Health In-formation	Personal data	Cardholder data

Control Structure	Risk-based con-trols (93 controls)	Trust Services Criteria	Administra-tive, Physi-cal, Tech-nical safe-guards	Principles-based privacy controls	12 prescrip-tive tech-nical re-quirements
Risk Man-agement	Mandatory	Required	Required	Implied	Required
Encryption	Recommended	Recommended	Addressable	Recommended	Mandatory
Logging & Monitoring	Yes	Yes	Yes	Limited	Mandatory
Incident Response	Required	Required	Required	Required	Required
Vendor / Third-party Secu-rity	Yes	Yes	Limited	Yes	Yes
Privacy Rights	Not explicit	Partial	Limited	Strong and ex-plicit	Not appli-cable
Certifica-tion / Attes-tation	Certification	Attestation	No certifi-cation	No certification	Compliance validation
Audit Au-thority	Accredited ISO auditors	CPA firms	HHS / OCR	Data Protection Authorities	Qualified Security Assessors (QSA)
Audit Fre-quency	Annual surveil-lance	Annual	On com-plaint / breach	On complaint / breach	Annual + quarterly scans
Validity Period	3 years	1 year	Ongoing	Ongoing	1 year
Penalties for Non-Compliance	None	None	Up to $1.5M per year	Up to €20M or 4% turnover	Fines, loss of card privileges
Implementation Complexity	Medium	Medium	High	High	Very High
Typical Use Case	Enterprise-wide security governance	Customer trust assurance	Healthcare data protection	Privacy and data protection	Payment processing security

As illustrated in Table I, organizations often fall under multiple compliance scopes simultaneously. This overlap requires coordinated governance strategies to manage security controls across different regulatory environments [14], [17].

B. Control Categories Comparison

Despite differences in governance structures, most information security compliance frameworks em-phasize a common set of foundational security control categories. These controls include access man-agement, encryption mechanisms, monitoring capabilities, and incident response procedures across organizational systems. Also play an important role in protecting sensitive information across digital infrastructures. Consequently, many frameworks incorporate similar control categories even when their regulatory objectives differ.

Access control mechanisms appear consistently across ISO/IEC 27001, SOC 2, HIPAA, GDPR, and PCI DSS frameworks [1], [2], [3], [4], [8].

These controls restrict unauthorized access to systems and pro-tect sensitive organizational information assets. Encryption and monitoring mechanisms further strengthen data protection by ensuring confidentiality and supporting continuous system oversight.

However, frameworks differ in how these controls are implemented and enforced across organizational environments. ISO/IEC 27001 and SOC 2 provide flexible governance models that allow organizations to tailor security controls based on their risk assessments. In contrast, PCI DSS defines prescriptive technical requirements that specify detailed implementation procedures for protecting payment card information [2]. Regulatory frameworks such as GDPR and HIPAA emphasize accountability and legal responsibility for safeguarding personal and healthcare data [3], [4].

C. Certification and Audit Comparison

Certification and audit mechanisms play an essential role in validating whether organizational security controls meet the requirements defined by information security compliance frameworks. Different frameworks adopt varying approaches to certification and compliance verification processes. These mechanisms help organizations demonstrate accountability and maintain regulatory compliance.

Con-sequently, certification structures differ across governance standards, regulatory frameworks, and in-dustry security programs.

ISO/IEC 27001 requires organizations to undergo formal certification audits conducted by accredited external auditors who evaluate the effectiveness of the Information Security Management System [1].SOC 2 operates through attestation reports issued by certified public accounting firms assessing internal control effectiveness

based on Trust Services Criteria [8].In contrast, regulatory frameworks such as HIPAA and GDPR enforce compliance through regulatory oversight and legal enforcement mechanisms rather than formal certification processes [3], [4].

V. Cyber Resilience Implications of Multi-Framework Compliance

Information security compliance frameworks play a significant role in strengthening organizational cyber resilience by promoting structured security governance and risk management practices across modern digital infrastructures. These frameworks guide organizations in implementing consistent secu-rity controls and monitoring mechanisms. Improved governance structures help security teams identify vulnerabilities earlier. As a result, organizations can respond to cyber threats more effectively.

Implementing multiple compliance frameworks often increases visibility into organizational security operations and regulatory obligations. Security teams gain clearer insight into system configurations, access controls, and monitoring practices.

This visibility supports faster detection of security incidents and improves response coordination. Re-search indicates that integrated governance strategies strengthen overall cyber security resilience with-in complex digital ecosystems [15], [19].

However, resilience benefits depend on effective coordination across different compliance frameworks. Organizations must therefore integrate security governance practices to avoid duplicated controls and ensure efficient compliance management across regulatory environments [14], [17].

VI. Challenges in Compliance Implementation

Organizations implementing multiple compliance frameworks often encounter operational challenges related to governance complexity, resource allocation, and coordination of security controls across different regulatory environments. Control duplication is a common challenge. Many frameworks re-quire similar safeguards but describe them using different terminology and documentation structures. This inconsistency increases administrative workloads and complicates security governance practices. Security teams must therefore carefully coordinate policies and controls to maintain consistent compli-ance across organizational infrastructures.

Another major challenge involves documentation and audit preparation activities required by different regulatory frameworks. Organizations must collect extensive evidence including policy documents, security logs, configuration records, and training documentation to demonstrate compliance during audits. Maintaining such documentation across dynamic cloud environments requires significant time, expertise, and organizational resources.

VII. Automation and AI-Enabled Compliance Operations

Automation technologies are increasingly transforming how organizations manage regulatory compli-ance across complex digital infrastructures and cloud computing environments. Many organizations now rely on automated tools to monitor configurations and track compliance evidence. These tools continuously evaluate security control status across distributed systems. Automation therefore reduces manual workloads and improves the accuracy of compliance reporting.

Artificial intelligence techniques extend these capabilities by analyzing system activity and identifying potential compliance risks. Machine learning models can process large volumes of system logs to de-tect anomalies and possible control failures. Such capabilities support continuous monitoring ap-proaches that strengthen governance visibility and operational cyber security resilience [12], [15].

Cloud platforms further enable automated compliance monitoring by integrating security tools directly into infrastructure management environments. These technologies help organizations track configura-tion changes and maintain security policies across dynamic cloud infrastructures. Consequently, auto-mation and AI together support more efficient and scalable compliance management in modern digital ecosystems [17].

VIII. Future Trends

Emerging technological developments are expected to reshape how organizations manage information security compliance across increasingly complex digital infrastructures and cloud computing environ-ments. Cloud platforms are gradually embedding automated compliance monitoring tools within infra-structure management services. These tools help organizations track configuration changes and main-tain security policies across

distributed environments. Automation therefore reduces manual compli-ance workloads and improves operational efficiency. Many organizations are exploring integrated compliance platforms that support continuous monitoring of security controls. Such platforms may simplify compliance management across multiple regulatory frameworks.

Artificial intelligence technologies are also expected to influence future compliance strategies. Ma-chine learning models can analyze system activity and detect potential security or compliance anoma-lies. These capabilities allow organizations to identify risks earlier and respond more quickly to securi-ty incidents. Consequently, future compliance programs will likely rely on automated monitoring and intelligent governance mechanisms to maintain effective cyber security resilience [12], [15].

IX. Proposed AI-Driven Compliance Framework

To address the challenges of multi-framework compliance and limited real-time monitoring capabilities, this study proposes an AI-driven compliance management framework designed for cloud-based envi-ronments. The proposed system integrates automation and machine learning techniques to enable con-tinuous compliance monitoring and efficient governance across multiple regulatory frameworks.

The architecture of the proposed system consists of four key components: data collection, compliance mapping engine, AI-based analysis module, and monitoring dashboard. The data collection layer gath-ers information from various sources, including system logs, cloud configurations, access control rec-ords, and network activity. These inputs provide real-time visibility into organizational security opera-tions.

The compliance mapping engine aligns collected data with the control requirements of multiple frame-works such as ISO/IEC 27001, GDPR, HIPAA, and PCI DSS. This component identifies overlapping controls and reduces duplication by creating a unified compliance model. It enables organizations to manage multiple regulatory requirements within a single governance structure.

The AI-based analysis module uses machine learning techniques to detect anomalies and potential compliance violations. For example, unusual login patterns or unauthorized access attempts can be identified by analyzing behavioral deviations in system logs. These anomalies are then mapped to spe-cific compliance requirements, allowing organizations to detect violations proactively rather than dur-ing periodic audits.

The monitoring dashboard provides real-time visualization of compliance status across systems. It highlights non-compliant controls, generates alerts, and assists security teams in prioritizing remedia-tion actions. This improves decision-making and reduces manual effort involved in compliance track-ing.

A typical use case of the proposed framework can be observed in a cloud-based healthcare system that must comply with both HIPAA and GDPR regulations. The system continuously monitors access to sen-sitive patient data, detects unauthorized access attempts using AI models, and maps these events to compliance requirements. This ensures timely detection and response to potential violations.

Overall, the proposed framework enhances compliance efficiency by reducing manual workload, im-proving real-time monitoring, and enabling proactive risk management. It aligns with modern cloud security practices and supports scalable compliance management in complex digital environments.

X. Conclusion

This study examined major information security compliance frameworks widely adopted across mod-ern digital environments and cloud computing infrastructures. The analysis compared their governance structures, regulatory characteristics, and implementation approaches. Despite their differences, these frameworks share fundamental cyber security objectives such as access control, monitoring, and inci-dent response, providing a foundation for coordinated security governance across organizations.

Multi-framework compliance has become a practical necessity in complex digital ecosystems. However, managing multiple frameworks introduces challenges related to control duplication, monitoring com-plexity, and resource overhead.

To address these challenges, this study proposed an AI-driven compliance framework that integrates automation and machine learning techniques for continuous monitoring and unified compliance man-agement. The proposed approach enhances visibility into security controls, enables proactive detection of compliance violations, and reduces manual effort in audit and reporting processes.

Future compliance strategies are expected to increasingly rely on intelligent and automated systems to improve governance efficiency and cyber security resilience. Such approaches will play a critical role in enabling scalable and adaptive compliance management in evolving cloud environments.

REFERENCES

[1] ISO/IEC 27001:2022, Information security, cyber security and privacy protection — Information security management systems — Requirements, International Organization for Standardization, 2022.
[2] PCI Security Standards Council, PCI DSS v4.0 Documentation, PCI SSC, 2022–2024.
[3] European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), Official Journal of the European Union, 2016.
[4] U.S. Department of Health & Human Services (HHS), The HIPAA Security Rule, HHS, 2003.
[5] National Institute of Standards and Technology, Security and Privacy Controls for Information Sys-tems and Organizations, NIST SP 800-53 Rev. 5, Sept. 2020.
[6] S. Mia, "A comparative study on HIPAA technical safeguards for mobile health applications," Computers & Security, 2022.
[7] T. R. McIntosh et al., "From COBIT to ISO 42001: Evaluating cyber security frameworks and readi-ness," Computers & Security, 2024.
[8] American Institute of Certified Public Accountants (AICPA), SOC 2®—Trust Services Criteria, AICPA, New York, NY, USA, 2017.
[9] SANS Institute, SANS 2023 SOC Survey, SANS Institute, 2023.
[10] European Data Protection Board, EDPB Annual Report 2022, 2023.
[11] P. K. Joshi, "Achieving PCI-DSS Compliance in Payment Gateways: A Comprehensive Approach," Journal of Technology and Systems, vol. 6, no. 7, pp. 13–31, Oct. 2024.
[12] S. Olatunji, "Automating compliance evidence extraction with machine learning," in Smart Sys-tems and Applications, Springer, 2024.
[13] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Insti-tute of Standards and Technology, 2018.
[14] Cloud Security Alliance, Cloud Controls Matrix (CCM) Version 4.0, CSA, 2021.
[15] S. Behl and K. Behl, "Cybersecurity governance and compliance frameworks in cloud computing environments," IEEE Access, vol. 11, pp. 75421–75439, 2023.
[16] ENISA, Cybersecurity Certification and EU Cybersecurity Act Overview, European Union Agency for Cybersecurity, 2022.
[17] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Data protection and cybersecurity compliance in cloud computing," Future Generation Computer Systems, vol. 97, pp. 308–321, 2019.
[18] A.Behl and A. Behl, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford Univer-sity Press, 2021.
[19] J. Rees, S. Bandyopadhyay, and E. H. Spafford, "A framework for cybersecurity compliance man-agement in enterprise systems," Information Systems Frontiers, vol. 23, no. 2, pp. 355– 372, 2021.
[20] Gartner, Market Guide for Integrated Risk Management (IRM) Solutions, Gartner Research, 2023.