2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity) | 979-8-3503-8952-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/BigDataSecurity62737.2024.00013

A Survey of Major Cybersecurity Compliance Frameworks

Wenjia Wang*, Seyed Masoud Sadjadi†, Naphtali Rishe‡
Knight Foundation School of Computing and Information Sciences
Florida International University
Miami, USA
Email:wwang048@fiu.edu*, sadjadi@cs.fiu.edu†, rishen@cs.fiu.edu‡

***Abstract*—Motivated by the challenge of navigating the complex landscape of cybersecurity compliance, this study critically examines and evaluates seven major cybersecurity frameworks: SOC 2, GDPR, PCI DSS, HIPAA, CIS Controls V8, NIST CSF, and CMMC 2.0. Our research focuses on understanding their distinct features and operational nuances, addressing a significant gap in current compliance strategies. We contribute a novel set of risk management-based evaluation criteria, offering a comprehensive analysis of these frameworks. The study further explores the Secure Controls Framework (SCF) and its effective integration with these frameworks, summarizing a unified mapping approach. This mapping facilitates streamlined compliance across multiple standards, providing a strategic tool for organizations. Our findings offer pivotal insights into the efficacy of each framework in managing cybersecurity risks, underlining the necessity for an integrated, risk-focused approach to compliance in the digital era.**

***Index Terms*— Cybersecurity, GRC, Compliance, SOC 2, GDPR, PCI DSS, HIPAA, CIS, NIST CSF, CMMC, SCF**

NOMENCLATURE

Governance, Risk, and Compliance (GRC), Service Organization Control 2 (SOC 2), General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Center for Internet Security (CIS), National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Cybersecurity Maturity Model Certification (CMMC), Secure Controls Framework (SCF)

I. INTRODUCTION

In today's rapidly evolving digital landscape, the expansive realm of cyberspace has become integral to our daily lives, underscoring the growing importance and heightened requirement for robust cybersecurity measures [1]. As our reliance on digital platforms escalates, with cybercrime rapidly emerging as a pervasive threat, the need for comprehensive, adaptive, and collaborative cybersecurity strategies becomes more critical [2] [3] [4]. In this context, the concepts of Governance, Risk, and Compliance (GRC) [5] have become pivotal in shaping organizational strategies, particularly in cybersecurity [6]. Governance ensures that organizational activities align with overall goals, the management of Risk involves identifying and mitigating potential threats, and Compliance, the cornerstone of our focus, ensures adherence to laws and regulations. This triad of GRC is critical in maintaining the integrity, security, and resilience of organizations in this digital age [7] [8] [9].

The role of Compliance within the GRC framework is particularly vital. It encompasses not just adherence to regulatory standards but also the strategic integration of these standards into the organization's cybersecurity practices [10]. Effective compliance means not only meeting legal requirements but also implementing and maintaining robust security measures [11].

As crucial as compliance is, it presents its own set of challenges. Businesses today are navigating an increasingly complex landscape of evolving cyber threats and stringent compliance requirements, facing not only the risk of data and property loss but also significant penalties for noncompliance [12] [13]. Compounding these issues is the challenge of aligning with multiple cybersecurity standards, which not only evolve independently but also often necessitate simultaneous adherence, adding layers of complexity to an already demanding compliance landscape [14]. Although a substantial body of work exists in the field of compliance, it falls short of comprehensively addressing all aspects of the compliance problem [15] [16], thereby underscoring the necessity for continued exploration and development in this area.

In this vein, our survey critically examines seven major compliance frameworks, namely SOC 2, GDPR, PCI DSS, HIPAA, CIS Control V8, NIST CSF, and CMMC 2.0. Our analysis extends beyond simple comparison as we introduce an original set of evaluation criteria tailored to assess these frameworks from a risk management perspective. This criteria set, a key contribution of our work, enables a comprehensive evaluation of each framework's capabilities in managing cybersecurity risks. Alongside this, in the course of this exploration, the Secure Controls Framework (SCF) surfaced as a comprehensive resource, providing a consolidated mapping of these compliance standards. This paper contributes an overview of the SCF and presents a distilled synthesis of its 33 domains as they relate to the seven frameworks, a summary that, while derived from the broader SCF community's efforts, represents another small novel work of this study.

Following this introduction, the paper is structured as follows: Section II explores relevant literature on cybersecurity compliance challenges and solutions. Section III examines

979-8-3503-8952-4/24/$31.00 ©2024 IEEE
DOI 10.1109/BigDataSecurity62737.2024.00013

seven key compliance frameworks, comparatively analyzing their features and interconnections. Section IV assesses the frameworks using a set of criteria developed from a risk management perspective. Section V delves into SCF, its goals, and its integration with other standards, summarizing its 33-domain mapping to the seven compliance frameworks discussed within the paper. Section VI summarizes our findings and their implications for the field. Finally, Section VII suggests avenues for future research.

II. Related Work

In reviewing related literature, we consider works that both identify the challenges in compliance and those that propose potential solutions or frameworks for these challenges.

[17] identify a significant gap in the availability of clear reference architectures and patterns for compliance, making it challenging for cloud service providers and consumers to achieve and maintain compliance, this gap is also what we are addressing in this paper. In BYOD (Bring your own device) security, organizations are also facing the same difficulty [18]. [19] summarized technical challenges in the implementation of Privacy Compliance. [20] underscores the complexity of compliance in modern digital environments. An architecture integrated with OpenStack was proposed in [21] to address the critical need for automated tools in verifying security compliance of cloud services.

After exploring the mediation effect of cooperation on the relationship between organizational practices and cybersecurity compliance, [22] emphasized the importance of top management commitment, structured security processes, and security investment in enhancing compliance through cooperative efforts in organizations. [23] found that users' compliance with security measures varies, with some motivated by instructions, others by evidence, and some by fear of sanctions or personal repercussions. [24] explores the transition of employee behavior from noncompliance to compliance with information security policies, highlighting that value conflicts and stress lead to noncompliance, while motivational factors promote compliance.

Cyber threats and compliance challenges are not only headaches for big companies but also bother SMEs (Small and Medium-Sized Enterprises) [25]. The study in [26] reviews the cyber security challenges of SMEs aligning with NIST CSF, finding that research primarily focuses on the Identify and Protect, with limited attention to Detect, Respond, and Recover aspects. [27] provide a comprehensive review of the challenges and factors influencing information security policies, underscoring the pivotal role of organizational and human factors in shaping compliance behaviors within organizations. Balozian and Leidner's study [28] delves into the determinants of information system security policy compliance in organizations, emphasizing the role of insider threats and the interplay of human and organizational factors critical to the efficacy of cybersecurity frameworks. For the same concern, the survey conducted in [29] suggests entities set "Chief Privacy Officer".

Due to the complexity and varying interpretations of compliance standards, entities also face challenges in large-scale software development compliance, such as interpreting abstractly written requirements, coordinating activities across multiple units, and resource constraints [30]. [31] provides a comprehensive comparison of goal-oriented and non-goal-oriented modeling methods in legal and regulatory compliance, highlighting the predominance of these methods in healthcare and privacy contexts and underscoring a need for more diverse application domains and a greater focus on analysis and enactment tasks in compliance modeling.

In exploring the landscape of cybersecurity compliance, a range of solutions have emerged, each addressing different facets of this complex domain.

A. AWS QuickStart Compliance Solutions

Amazon Web Services (AWS) offers a range of QuickStart solutions designed to assist organizations in achieving compliance with specific regulatory standards within its cloud environment [32]. Notably, AWS provides CloudFormation templates for major compliances such as PCI DSS [33] and HIPAA [34]. These templates help automate the setup of AWS environments in a way that meets the stringent requirements of these standards. The solutions utilize a defined toolset from AWS to streamline the compliance process. However, they are geared specifically towards AWS cloud services and can only address one compliance standard at a time. Additionally, the cost can be significant due to the reliance on AWS's toolset. While these solutions are efficient within the AWS ecosystem, their utility is limited for organizations operating outside of AWS or in multi-cloud and hybrid environments.

B. RapidFire Tools for GRC

RapidFire Tools offers a comprehensive suite of (GRC) management solutions designed to streamline the process of cybersecurity assessment and compliance [35]. It presents an overview of an organization's adherence to various compliance frameworks like CIS Controls, HIPAA, and PCI DSS. Users can evaluate their compliance status through visual indicators that summarize the percentage of standards covered, the progress of baseline assessments, and the thoroughness of requirement assessments. The tool's design facilitates not just a high-level overview but also a granular, in-depth look at compliance metrics. It translates complex regulatory requirements into actionable insights, enabling organizations to maintain stringent security standards and remain compliant with evolving regulations.

Despite these advancements, a significant gap remains in the literature and solutions - a unified approach to multi-standard compliance. AWS QuickStart's drawback lies in its broad focus which, while offering wide-ranging solutions, can lack specificity for nuanced compliance scenarios, and RapidFire Tools, though meticulous in detailing individual compliance criteria, lacks an integrated approach to interlink compliance efforts across different organizational roles or departments. In short, current tools and methodologies predominantly focus

on singular compliance standards or specific industry needs. There is a clear need for a more inclusive framework that can handle the complexities of multiple compliance standards simultaneously.

III. Overview of the Seven Major Compliance Frameworks

In this section, we systematically examine seven key cybersecurity compliance frameworks, employing a uniform analytical approach to assess their distinctive characteristics and common features. Our focused analysis highlights their objectives, scopes, and operational details, aiming to reveal both the unique and shared elements across these frameworks. This comparative dissection is essential for understanding how each framework individually and collectively strengthens cybersecurity strategies. By distilling these frameworks into core components, we lay the groundwork for a more detailed evaluation in Section IV and integrating them into a comprehensive, unified cybersecurity approach in Section V.

Before we dive into the nuances of each compliance framework, it's important to highlight their core requirement types, which can be broadly categorized into three: Statutory, Regulatory, and Contractual [36].

- Statutory Requirements are laws passed by legislative bodies, such as state or federal governments. They tend to be more static, changing primarily through new legislative actions.
- Regulatory Requirements are established by regulatory agencies under the government's authority. These requirements are more dynamic, evolving to address new challenges in the regulatory landscape.
- Contractual Requirements stem from agreements between private entities. These include specific cybersecurity or privacy stipulations agreed upon as part of their business relationships.

TABLE I
Compliance Requirement Types

Framework	Statutory	Regulatory	Contractual
SOC 2			✓
GDPR		✓	
PCI DSS			✓
HIPAA	✓		
CIS Controls V8			✓
NIST CSF		✓	
CMMC			✓

The comprehension of these requirement types can illuminate the legal and operational frameworks within which each compliance standard operates. Table I shows the requirement types of the compliances discussed in this paper. This understanding is instrumental in strategically applying these standards to reinforce cybersecurity and data protection measures.

A. SOC 2 (Trust Services Criteria)

Service Organization Control Type 2 (SOC 2), developed by the American Institute of Certified Public Accountants (AICPA), is a pivotal framework in cybersecurity, specially designed for managing and safeguarding data critical to an organization's privacy and confidentiality [37]. SOC 2 compliance is structured around two main components: Trust Services Criteria (TSC) and SOC 2 reports.

1) Objective: SOC 2's primary objective is to ensure the secure management and safeguarding of data in third-party service providers.

2) Trust Services Criteria: The TSC are the foundational elements of SOC 2 compliance, providing a structured set of standards and principles that directly inform and shape the requirements and assessments within the SOC 2 framework. These criteria encompass key areas of cybersecurity and operational integrity, serving as the benchmark against which organizations' control mechanisms are evaluated for SOC 2 compliance. TSC are classified into the following categories:

- **Security**: Incorporates access control and protection of information system resources against unauthorized access.
- **Availability**: Ensures system operations are reliably available and incidents are effectively managed.
- **Processing Integrity**: Guarantees system processing is complete, valid, accurate, timely, and authorized, with data integrity maintained throughout.
- **Confidentiality**: Focuses on encrypting and restricting access to confidential information.
- **Privacy**: Protects personal information and ensures disclosure complies with legal and agreed-upon requirements.

3) Entities Covered: Primarily applicable to technology and cloud computing organizations, SOC 2 is critical for entities handling client information, especially for SaaS businesses and technology companies managing significant customer data volumes.

4) SOC 2 Reports: These reports are crucial in evaluating a service organization's security posture. Prepared by external auditors, SOC 2 reports verify the effectiveness of internal controls based on the TSC. These reports not only reinforce client and stakeholder confidence but also ensure adherence to stringent data protection standards. SOC 2 Reports are categorized into two types:

- Type I report evaluates the design of controls at a specific point, focusing on their suitability and alignment with the trust criteria.
- Type II report assesses the operational effectiveness of these controls over a period (typically six months), verifying their practical performance in data protection and system reliability.

5) Implementation and Challenges: Implementing SOC 2 involves addressing common challenges such as aligning the framework with business objectives, training employees, and regularly updating practices to match evolving threats. Organizations should adopt a proactive approach, continuously reviewing and improving their security measures to remain compliant.

6) Comparative Analysis: Compared to frameworks like ISO 27001 or HIPAA, SOC 2 offers a more tailored approach for service organizations, particularly those in cloud computing and SaaS sectors. Its emphasis on specific TSC makes it a comprehensive choice for these entities.

7) Impact of Noncompliance: Noncompliance with SOC 2 can lead to significant legal, financial, and reputational risks, emphasizing the framework's importance in the modern cybersecurity ecosystem.

SOC 2 stands as a critical framework for technology and cloud computing organizations, necessitating stringent information security policies and procedures to ensure the confidentiality, integrity, and availability of customer data. Its rigorous requirements and detailed reporting process ensure that organizations maintain high standards of security and operational excellence.

B. GDPR

The General Data Protection Regulation (GDPR), implemented by the European Union (EU), effective from May 25, 2018, marks a major overhaul in data protection laws, standardizing regulations across EU states to boost privacy rights and transform how organizations handle data privacy. It impacts any entity dealing with EU residents' data, regardless of the organization's location [38].

1) Objective: GDPR's fundamental goal is to empower individuals with greater control over their personal data, ensuring robust protection across various sectors.

2) Technology Adaptation: GDPR is designed to adapt to technological advancements. It addresses modern data handling methods like online behavior tracking, the use of cookies, and other monitoring technologies, ensuring that data protection measures stay effective as technology evolves.

3) Key Entities in GDPR:

- **Data Subjects**: Individuals (primarily EU citizens or residents) whose data is processed. Their enhanced rights under GDPR include access, rectification, erasure, restriction, objection to processing, and data portability.
- **Data Controllers**: Entities deciding the purposes and means of processing personal data.
- **Data Processors**: Entities processing data on behalf of Data Controllers.

4) Key Data Processing Principles: GDPR mandates adherence to principles like lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality in data processing.

- **Lawfulness, Fairness, and Transparency**: Data processing should be legal, fair, and transparent to Data Subjects.
- **Purpose Limitation**: Data must be collected for specific, legitimate purposes and not processed further in incompatible ways.
- **Data Minimization**: Only necessary data should be collected.
- **Accuracy**: Data must be accurate and kept up-to-date.
- **Storage Limitation**: Data shouldn't be retained longer than necessary.
- **Integrity and Confidentiality**: Data must be processed securely to prevent unauthorized access and loss.

5) Key Operational Requirements:

- **Breach Notification**: Organizations must notify relevant authorities and affected Data Subjects within 72 hours of a data breach.
- **Expertise**: Organizations should have expertise in data protection, including appointing a Data Protection Officer (DPO).
- **Accountability and Governance**: Organizations must implement governance measures for data protection and demonstrate compliance.

6) Special Categories of Data: GDPR identifies sensitive data categories (e.g., racial or ethnic origin, political opinions, religious beliefs, genetic data, etc.) and imposes stringent conditions on their processing.

7) Implementation and Challenges: The complexities of implementing GDPR include integrating GDPR requirements into existing data management practices, ensuring continuous compliance, and adapting to evolving interpretations of privacy regulations. Challenges also arise from the need to comprehensively understand the scope of data collected, processed, and stored, as well as ensuring robust data protection and breach response mechanisms. Additionally, organizations face the task of training employees about GDPR compliance and raising awareness about data subjects' rights.

8) Comparative Analysis: Unlike regulations that may focus solely on specific sectors (like HIPAA in healthcare) or have a more limited geographical scope, GDPR applies to any entity processing the data of EU residents, making it more globally encompassing. It also sets a higher standard for consent and data subject rights, offering a more holistic approach to data protection than many other frameworks.

9) Impact of Noncompliance: The consequences of noncompliance with GDPR are significant, potentially leading to severe financial penalties, legal actions, and reputational damage. Fines can reach up to €20 million or 4% of the annual global turnover, whichever is higher, representing a substantial financial risk. Beyond monetary penalties, noncompliance can also lead to a loss of consumer trust, damage to brand reputation, and long-term operational disruptions.

C. PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS), established by the PCI Security Standards Council formed by major credit card companies like Visa, MasterCard, American Express, Discover, and JCB, aims to protect cardholder data and secure payment card transactions globally. Since its inception in 2004, PCI DSS sets out technical and operational requirements for all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers [39].

1) Objective: PCI DSS revolves around six key objectives, comprising a total of 12 specific requirements. These objectives include building and maintaining secure network

systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

2) Self-Assessment Questionnaires (SAQs): SAQs are tools for merchants and service providers to self-assess their PCI DSS compliance. Various types of SAQs address different business models and risk postures, ranging from those for merchants entirely outsourcing cardholder data functions (SAQ A) to those processing transactions on-site (SAQ D Merchant).

Among the SAQs, the most comprehensive one is SAQ D. SAQ D is intended for merchants and service providers who do not fall into the categories covered by the other SAQ types. It covers all the PCI DSS requirements and is therefore the broadest in scope.

3) Levels of PCI DSS Compliance: Merchants are categorized into four levels based on annual transaction volume, each with specific compliance validation requirements. These levels range from Level 1 merchants processing over 6 million transactions to Level 4 merchants with fewer transactions.

4) Implementation and Challenges: Implementing PCI DSS involves addressing various challenges, such as understanding and integrating the requirements into existing systems, ensuring continuous compliance, and adapting to evolving payment technologies. Challenges also include training staff, securing cardholder data in diverse processing environments, and meeting the specific requirements of different merchant levels.

5) Comparative Analysis: Compared to other data security standards, PCI DSS is unique in its specific focus on payment card and cardholder data security. While frameworks like GDPR and HIPAA govern broader data privacy concerns, PCI DSS zeroes in on the unique vulnerabilities of payment card transactions, offering a targeted approach to securing cardholder data in a variety of transaction environments.

6) Impact of Noncompliance: Noncompliance with PCI DSS can result in significant consequences, including financial penalties, increased transaction fees, and reputational damage. In severe cases, it can lead to the loss of card processing capabilities. The repercussions emphasize the need for robust compliance to safeguard against data breaches and maintain consumer trust.

D. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is crucial U.S. legislation that governs the security and privacy of health records, focusing on Protected Health Information (PHI) and Electronic Protected Health Information (ePHI). HIPAA is mandatory for all healthcare organizations in the United States [40].

1) Objective: HIPAA aims to safeguard the confidentiality, integrity, and availability of PHI and ePHI, covering a broad spectrum of health-related information.

2) Entities Covered: HIPAA applies predominantly to healthcare providers, health insurance plans, healthcare clearinghouses, and business associates handling PHI on their behalf.

3) Structure and Key Rules:

- **Privacy Rule**
  - *Disclosure*: Requires covered entities to inform individuals about their privacy practices initially.
  - *Permitted Uses*: Outlines specific allowable uses of PHI, including treatment and payment, with other uses requiring explicit consent.
  - *Protection Measures*: Mandates controls to maintain PHI's confidentiality and integrity.
- **Security Rule**
  - *Applicability*: Focuses on securing ePHI.
  - *Protection*: Requires the protection of ePHI's confidentiality, integrity, and availability.
  - *Workforce Compliance*: Ensures compliance with the rule's provisions by the workforce of covered entities.
  - *Transactions*: Applies to various electronic healthcare transactions.
- **Breach Notification Rule**
  - Mandates notification to affected individuals and HHS within 60 days following a breach involving unsecured PHI.

4) Implementation and Challenges: Implementing HIPAA involves integrating its comprehensive requirements into the healthcare organization's practices, ensuring compliance across all operations involving PHI and ePHI. Challenges include maintaining up-to-date knowledge of regulatory changes, ensuring workforce compliance, and effectively managing business associate relationships.

5) Comparative Analysis: Compared to other compliance frameworks, HIPAA is unique in its specific focus on the healthcare sector and its comprehensive coverage of both PHI and ePHI. While frameworks like GDPR and PCI DSS have broader applicability, HIPAA specifically addresses the nuances of healthcare information, emphasizing patient privacy and data security in a healthcare context.

6) Impact of Noncompliance: Noncompliance with HIPAA can result in significant civil monetary penalties, ranging from $137 to $68,928 per violation based on culpability [41]. It also poses a risk to an organization's reputation, potentially leading to a loss of trust among patients and partners.

E. CIS Controls V8

Developed by the Center for Internet Security since 2008 and updated in 2021 to version 8, the CIS Controls provide a strategic framework of 18 critical cybersecurity actions tailored for the modern digital landscape [42].

1) Key Focus Areas: CIS Controls V8 encompasses a range of focus areas, including:

- Inventory and Control of Hardware and Software Assets: Tracking and managing devices and software to secure the network.
- Data Protection: Safeguarding sensitive information through controlled access and secure storage practices.
- Secure Configuration: Ensuring systems and software are securely configured to mitigate vulnerabilities.

- Vulnerability Management: Continuously identifying and addressing system and software vulnerabilities.
- Incident Response: Preparing and managing effective responses to security breaches.
- Additional controls covering account management, access control, network and wireless security, email and web browser protections, malware defenses, and more.

2) Implementation Groups: CIS Controls V8 introduces three Implementation Groups (IGs) to cater to organizations at different levels of cybersecurity maturity:

- IG1 (Basic): Essential controls for all organizations to establish basic cybersecurity hygiene.
- IG2 (Foundational): Additional controls for organizations with moderate cybersecurity maturity, looking to enhance their defenses.
- IG3 (Advanced): Advanced practices for highly mature organizations seeking comprehensive cybersecurity measures.

3) Adaptation and Progression: The structure of CIS Controls V8 allows organizations to adapt and progress their cybersecurity measures. Starting with IG1, organizations can gradually implement more advanced controls (IG2 and IG3) as they evolve, ensuring continuous improvement and adaptation to new threats and technologies.

4) Implementation and Challenges: Implementing CIS Controls V8 involves assessing an organization's current cybersecurity posture, prioritizing controls based on risk assessment, and continuously adapting to emerging threats. Challenges include resource allocation, maintaining up-to-date knowledge of evolving threats, and ensuring organization-wide adherence to these controls.

5) Comparative Analysis: CIS Controls V8 stands distinct from regulatory frameworks like HIPAA or GDPR, which are legally binding and specific to health data privacy and general data protection, respectively. In contrast, CIS Controls V8 offers a set of voluntary best practices applicable across all sectors and industries. Compared to SOC 2 and PCI DSS, which are tailored for service organizations and payment card security, respectively, CIS Controls V8 provides a more generalized, comprehensive set of guidelines that can be adapted by any organization, regardless of its size or industry. This universality and adaptability make CIS Controls V8 a versatile tool for enhancing cybersecurity measures across a wide range of operational contexts.

6) Impact of Noncompliance: While noncompliance with CIS Controls V8 does not incur legal penalties like HIPAA or GDPR, failure to adhere can lead to increased vulnerability to cyberattacks, potential data breaches, and associated reputational and financial damages.

F. NIST CSF

The NIST Cybersecurity Framework is a comprehensive guideline established to assist organizations in managing cybersecurity risks. It includes standards, guidelines, and best practices adaptable across various industries, making it a flexible tool for enhancing cybersecurity measures [43] [44].

1) Objective: NIST CSF aims to enhance cybersecurity risk management, especially within critical infrastructure sectors. It focuses on safeguarding the confidentiality, integrity, and availability of information.

2) Main Components: NIST CSF is composed of three primary elements: the Core, Profiles, and Implementation Tiers. These components together provide a comprehensive approach for organizations to establish or enhance their cybersecurity risk management program. This includes prioritizing and scoping activities, orienting towards a cybersecurity risk management mindset, developing current and target profiles, conducting risk assessments, analyzing gaps, and implementing strategic action plans.

- **Core:** The Core of the NIST CSF is divided into five primary functions: Identify, Protect, Detect, Respond, and Recover. Each function is further broken down into categories and subcategories, offering detailed guidance on various aspects of cybersecurity.
- **Profile:** NIST CSF Profiles help organizations tailor their cybersecurity measures to their specific needs and goals. They facilitate the alignment of cybersecurity activities with business objectives, risk appetite, and resources.
- **Implementation Tiers:** The framework's Implementation Tiers (Partial, Risk Informed, Repeatable, and Adaptive) serve as benchmarks for assessing an organization's cybersecurity maturity and guiding its progress.

3) Implementation and Challenges: Implementing NIST CSF involves integrating it into existing organizational processes, which can be challenging due to resource constraints and the need for continuous adaptation to emerging threats.

4) Comparative Analysis: Unlike compliance-driven frameworks like HIPAA or GDPR, NIST CSF is a set of voluntary best practices applicable across sectors. It offers more flexibility compared to industry-specific standards like SOC 2 or PCI DSS, providing a broader approach to managing cybersecurity risks.

5) Impact of Noncompliance: While NIST CSF is a voluntary framework and noncompliance does not incur legal penalties, failure to adhere can result in increased cybersecurity risks, potential data breaches, and associated operational and reputational damages.

G. CMMC 2.0

The Cybersecurity Maturity Model Certification (CMMC) 2.0, developed by the U.S. Department of Defense (DoD) for the Defense Industrial Base (DIB), aims to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), improving cybersecurity practices across the defense supply chain [45] [46].

1) Objective: CMMC 2.0 focuses on protecting the confidentiality and integrity of FCI and CUI from unauthorized access and modification. It is a mandatory compliance requirement for organizations seeking to participate in DoD contracts.

2) Key Features: CMMC 2.0 streamlines the certification process with three levels, each aligned with NIST cybersecurity standards:

- Level 1 (Foundational): Addresses basic cybersecurity practices to protect FCI.
- Level 2 (Advanced): Aligns with NIST SP 800-171, covering enhanced cybersecurity practices.
- Level 3 (Expert): Incorporates sophisticated practices based on a subset of NIST SP 800-172 requirements.

3) Assessment Requirement: CMMC 2.0 emphasizes verification through assessments, ensuring organizations meet necessary cybersecurity criteria.

4) Third-party Assessors: Certification involves CMMC Third Party Assessor Organizations (C3PAOs) responsible for evaluating compliance.

5) Domain Structure: CMMC 2.0 encompasses 14 core security domains, aligning with NIST SP 800-171. These domains include Access Control, Incident Response, Risk Assessment, and others.

6) Implementation and Challenges: Implementing CMMC 2.0 presents challenges such as understanding and integrating the specific requirements at each level, ensuring continuous compliance, and preparing for assessments. Smaller organizations may face resource constraints, while all need to stay updated with evolving cybersecurity standards.

7) Comparative Analysis: CMMC 2.0 incorporates practices and processes from various cybersecurity standards, including NIST SP 800-171, which is also a core component referenced in NIST CSF. Thus, organizations following NIST CSF may find some alignment and familiarity when aiming for CMMC certification, as both frameworks share common cybersecurity standards and best practices. While NIST CSF provides a flexible framework for managing cybersecurity risks across various contexts, CMMC 2.0 is specific to DoD contractors, focusing on protecting CUI within the defense sector.

8) Impact of Noncompliance: Noncompliance with CMMC 2.0 can result in losing eligibility for DoD contracts, which could have significant financial and strategic implications for businesses within the DIB. This underlines the critical importance of meeting CMMC standards for organizations in the defense supply chain.

IV. Evaluation of Cybersecurity Compliance Frameworks

In this section, we present a pivotal contribution of our study, wherein we introduce a novel set of evaluation criteria specifically designed for cybersecurity compliance frameworks. Subsequently, we embark on the evaluation of seven major frameworks: SOC 2, GDPR, PCI DSS, HIPAA, CIS Controls, NIST CSF, and CMMC 2.0, presenting our findings.

A. Evaluation Criteria

Our evaluation employs a set of rigorously defined criteria, developed with a strong emphasis on risk management. These criteria are inspired by two influential sources: the established framework evaluation approach proposed in [47] and the foundational concepts from [48]. While [47] offers a broad lens for framework evaluation, our approach tailors this perspective to align specifically with risk management, recognizing that compliance frameworks are fundamentally designed for managing and mitigating risk.

The intricate relationship between risk management and cybersecurity compliance frameworks forms the bedrock of our evaluation criteria. These frameworks are fundamentally designed to mitigate risks in the digital domain, safeguarding information assets while ensuring regulatory and ethical adherence. Effective risk management within these frameworks is pivotal, as it directly influences an organization's ability to protect against cyber threats, manage vulnerabilities, and respond to the dynamic nature of digital risks. Our criteria, therefore, are specifically tailored to probe the depth and breadth of each framework's risk management capabilities. By evaluating these frameworks through the lens of risk management, we gain crucial insights into how effectively they identify, assess, respond to, and monitor cybersecurity risks. This perspective is essential for understanding the real-world efficacy of these frameworks in protecting digital assets and maintaining cyber resilience. Our criteria not only serve as a tool for comparative analysis but also as a guide for organizations to discern which frameworks align best with their specific risk management needs and objectives. This approach underscores the indispensable role of risk management in shaping robust, adaptive, and proactive cybersecurity strategies.

Below are all 24 sub-criteria organized under the 12 main criteria:

1) **Risk Identification** - Does the framework have clearly defined principles or points focusing on identifying threats and measures to locate and mitigate these threats?
   1. Threat Identification - Does the framework have clear guidelines for identifying and documenting potential threats to the organization's digital assets?
   2. Asset Identification - Does the framework provide methods for enumerating and classifying organizational assets susceptible to cyber threats?
2) **Risk Assessment** - Does the framework include processes for evaluating the potential impact and likelihood of identified risks?
   1. Impact Analysis - Does the framework include mechanisms for analyzing the potential consequences of cybersecurity incidents?
   2. Likelihood Assessment - Does the framework offer methodologies for estimating the probability of risk occurrences?
3) **Risk Response** - Does the framework outline strategic options and plans for addressing and mitigating identified risks?
   1. Mitigation Strategies - Does the framework provide strategic options for reducing the impact or likelihood of risks?
   2. Incident Response Planning - Does the framework include guidelines for developing and implementing plans to address cybersecurity incidents?

4) **Risk Monitoring** - Does the framework support ongoing observation, tracking, and reporting of cybersecurity posture and risks?
    1. Continuous Monitoring - Does the framework facilitate continuous monitoring and reporting of the cybersecurity posture?
    2. Review and Update - Does the framework include procedures for periodic review and update of risk monitoring mechanisms?
5) **Business Continuity Integration** - Does the framework integrate cybersecurity risk management into broader business continuity planning?
    1. Integration with Business Processes - Is the framework aligned with organizational processes for seamless risk management integration?
    2. Disaster Recovery Planning - Does the framework provide planning and execution guidelines for recovery from cybersecurity incidents?
6) **Compliance Alignment** - Does the framework adhere to legal, statutory, and regulatory cybersecurity mandates?
    1. Legal Compliance - Is the framework in line with statutory cybersecurity obligations?
    2. Regulatory Compliance - Does the framework conform to cybersecurity regulations imposed by governing bodies?
7) **Best Practices and Standards** - Does the framework reflect established cybersecurity best practices and industry standards?
    1. Industry Standards Alignment - Is the framework consistent with recognized cybersecurity standards?
    2. Best Practice Guidance - Does the framework recommend best practices in cybersecurity risk management?
8) **Training and Awareness** - Does the framework provide educational resources and strategies for enhancing stakeholder cybersecurity awareness?
    1. Employee Training Programs - Does the framework offer training resources to enhance employee cybersecurity awareness?
    2. Stakeholder Awareness - Are there strategies within the framework for raising cybersecurity risk awareness among all stakeholders?
9) **Resource Allocation** - Does the framework guide the allocation of financial and human resources for effective cybersecurity risk management?
    1. Financial Resource Allocation - Does the framework advise on budgeting for cybersecurity measures?
    2. Human Resource Allocation - Are there recommendations within the framework for staffing and human resource investment in cybersecurity?
10) **Risk Reporting** - Does the framework establish risk communication channels and reporting protocols?
    1. Reporting Mechanisms - Is there a system within the framework for reporting cybersecurity risks and incidents?
    2. Stakeholder Communication - Does the framework include a process for informing stakeholders about the status of cybersecurity risks?
11) **Third-Party Risk Management** - Does the framework address risks associated with external parties and vendors?
    1. Vendor Risk Assessment - Are there guidelines within the framework for assessing and managing risks from third-party service providers?
    2. Contractual Risk Management - Does the framework incorporate mechanisms for risk management into contractual agreements?
12) **Maturity and Improvement** - Does the framework support the assessment and evolution of cybersecurity risk management processes?
    1. Maturity Assessment Tools - Are there tools within the framework for evaluating the maturity of an organization's cybersecurity practices?
    2. Improvement Roadmap - Does the framework provide guidance for developing a continuous cybersecurity improvement pathway?

B. Methodology

The evaluation of the compliance frameworks against the specified criteria involves a thorough analysis of the official documentation, guidelines, and standards associated with each framework. Here's a breakdown of how we operate:

1) Review of Official Documentation: For each compliance framework, the primary source of information is their official documentation. This includes guidelines, standards, and specifications published by the governing bodies or organizations responsible for the frameworks:

- SOC 2: Review of the TSC and the structure of SOC 2 reports.
- GDPR: Examination of the EU's official legal texts and guidelines regarding GDPR.
- PCI DSS: The evaluation of PCI DSS was based on the standard SAQ D provided by the PCI Security Standards Council since SAQ D covers all the PCI DSS requirements and is, therefore, the broadest SAQ in scope.
- HIPAA: Scrutiny of the HIPAA Rules (Privacy, Security, and Breach Notification) and related guidelines from the U.S. Department of Health & Human Services.
- CIS Controls V8, NIST CSF, CMMC 2.0: Evaluation based on the official publications from the Center for Internet Security, the National Institute of Standards and Technology, and the U.S. Department of Defense, respectively.

2) Evaluation Against Criteria: Each framework is evaluated against the 24 subcriteria to determine whether it has provisions, guidelines, or requirements that align with each criterion. Based on the analysis, a value is assigned to each criterion for each framework:

- True: The framework clearly and directly addresses the criterion.
- False: The framework does not address the criterion, or it is explicitly excluded.
- Partly: The framework addresses some aspects of the criterion but not comprehensively.
- Unclear: There is insufficient information, or it is ambiguous whether the framework addresses the criterion.

C. Results

Each of these criteria was applied to evaluate seven major cybersecurity compliance frameworks; a detailed view of how these frameworks align with each criterion is gathered in Table II. The evaluation results shown in Table II offer valuable insights for practitioners, highlighting the strengths and areas for improvement within each framework.

The majority of the frameworks scored 'True' across most criteria, indicating a strong alignment with risk management best practices in cybersecurity. This consistency reflects a comprehensive approach to threat identification, risk assessment, risk response, and risk monitoring, which are fundamental aspects of effective cybersecurity management.

Practitioners can use this table to select the most appropriate framework(s) based on their specific risk management needs and the strengths of each framework. The results also help organizations identify areas within their chosen framework(s) that may require additional focus or supplementation with other practices or standards. At the same time, the varying degrees of maturity and adaptability across frameworks highlight the importance of continual assessment and adaptation of cybersecurity practices to evolving threats and business needs.

Overall, this methodical evaluation serves as a valuable tool for organizations seeking to understand and select the most suitable cybersecurity compliance frameworks that align with their risk management practices and cybersecurity needs.

V. Analyzing and Mapping of the Secure Controls Framework

The Secure Controls Framework (SCF) is a comprehensive catalog of cybersecurity and data privacy controls. It's designed to help organizations develop, build, and maintain secure systems, processes, and applications. The SCF is more than just a collection of controls; it includes cybersecurity and privacy-related policies, standards, procedures, and technologies.

A. Overview

1) Purpose: The SCF acts as a meta-framework, a "framework of frameworks" that aids organizations in addressing a range of statutory, regulatory, and contractual requirements. It's developed to provide a unified approach to managing cybersecurity and data privacy, simplifying compliance for organizations subjected to various regulations [49].

2) Structure: The SCF is organized into 33 domains, 1,175 controls. These domains create a logical structure for discussing and implementing controls within and between organizations. The SCF aims to provide a shared set of controls to enhance governance practices and strengthen the overall state of security and privacy [50].

3) Key Features:

1) Comprehensive Catalog: The SCF offers a vast array of controls, guiding organizations in various aspects of cybersecurity and data privacy.
2) Integration with Operational Needs: The framework is designed to align with an organization's strategic, operational, and tactical requirements, regardless of its size or industry.
3) Flexibility and Adaptability: The SCF is flexible and can be adapted to meet the specific needs and compliance requirements of different organizations.
4) Focus on Collaboration: Emphasizing the importance of information sharing among cybersecurity professionals, the SCF encourages a collaborative approach to improve security and privacy practices.

4) Implementation and Application: Organizations can implement the SCF by downloading its content and tailoring the controls to their specific needs. It offers a practical approach to building a security program, with controls acting as building blocks to create a comprehensive cybersecurity and data privacy strategy. The framework also provides guidance on tools and solutions to address controls and contains maturity criteria to help organizations plan and evaluate controls based on their target maturity level.

5) Continuous Improvement: The framework is maintained by a community of experts and is continuously updated to reflect the evolving threat landscape, emerging technologies, and changes in regulatory requirements. This ensures that organizations adopting SCF are always at the forefront of best practices in cybersecurity and privacy.

6) Analysis:

- **Pros:** Provides a unified approach to managing diverse compliance requirements. Offers flexibility and adaptability to various organizational sizes and industries. Continuously updated by a community of experts to reflect current best practices.
- **Cons:** The extensive scope may be overwhelming for initial implementation. Potential overlap with existing controls in organizations with established compliance processes.

B. Mapping

In our endeavor to streamline the process of cybersecurity compliance, we have drawn upon the groundwork laid by the SCF community [51]. Their detailed work forms the bedrock of our summarized mapping, which effectively simplifies the alignment of SCF domains with seven major compliance frameworks discussed in this paper: SOC 2, GDPR, PCI DSS, HIPAA, CIS Controls V8, NIST CSF, and CMMC 2.0.

TABLE II
COMPREHENSIVE COMPARATIVE ANALYSIS OF CYBERSECURITY COMPLIANCES

#	Main Criteria	Sub-Criteria	SOC 2	GDPR	PCI DSS	HIPAA	CIS Controls V8	NIST CSF	CMMC 2.0
1	Risk Identification	1.1 Threat Identification	True	True	True	True	True	True	True
		1.2 Asset Identification	True	True	True	True	True	True	True
2	Risk Assessment	2.1 Impact Analysis	True	True	True	True	True	True	True
		2.2 Likelihood Assessment	True	True	Partly	False	False	True	False
3	Risk Response	3.1 Mitigation Strategies	True	True	True	True	True	True	True
		3.2 Incident Response Planning	True	True	True	True	True	True	True
4	Risk Monitoring	4.1 Continuous Monitoring	True	True	True	True	True	True	True
		4.2 Review and Update	True	True	True	True	True	True	True
5	Business Continuity Integration	5.1 Integration with Business Processes	True	True	True	True	True	True	True
		5.2 Disaster Recovery Planning	True	False	True	True	True	True	True
6	Compliance Alignment	6.1 Legal Compliance	True	True	True	True	True	True	True
		6.2 Regulatory Compliance	True	True	True	True	True	True	True
7	Best Practices and Standards	7.1 Industry Standards Alignment	True	True	True	True	True	True	True
		7.2 Best Practice Guidance	True	True	True	True	True	True	True
8	Training and Awareness	8.1 Employee Training Programs	True	True	True	True	True	True	True
		8.2 Stakeholder Awareness	True	True	True	True	True	True	True
9	Resource Allocation	9.1 Financial Resource Allocation	False	Partly	Partly	Partly	Partly	Unclear	Partly
		9.2 Human Resource Allocation	Partly	True	Partly	True	True	True	True
10	Risk Reporting	10.1 Reporting Mechanisms	True	True	True	True	True	True	True
		10.2 Stakeholder Communication	True	True	True	True	True	True	True
11	Third-Party Risk Management	11.1 Vendor Risk Assessment	True	True	True	True	True	True	True
		11.2 Contractual Risk Management	True	True	True	True	True	True	True
12	Maturity and Improvement	12.1 Maturity Assessment Tools	Partly	Unclear	False	False	False	True	True
		12.2 Improvement Roadmap	Partly	Unclear	False	False	Partly	True	True

This summarized mapping, detailed in Table III, serves as a tool for organizations to achieve compliance across multiple frameworks efficiently. By identifying overlapping SCF domains and controls, organizations can focus on key areas, significantly reducing the complexity and costs associated with compliance.

For an in-depth exploration of the SCF and its comprehensive mapping, the complete list of 1175 SCF controls and their association with the frameworks can be found on our GitHub repository: SCFMapping [52].

This synthesis not only condenses the information into a more user-friendly format but also underscores the practical advantages of this approach—by complying with overlapping domains and controls within the SCF, organizations can ensure adherence to multiple compliance standards simultaneously. This strategic focus streamlines compliance efforts, leading to a fortified and more integrated cybersecurity posture.

VI. CONCLUSION

This paper analyzes and evaluates major cybersecurity compliance frameworks, driven by the objective of identifying and addressing the challenges within the compliance domain. Our development of unique risk management-based criteria has illuminated the efficacy and limitations of each framework in managing cyber risks and meeting compliance demands. By integrating these frameworks with the SCF's mapping, we provide a strategic approach for organizations to simultaneously adhere to multiple compliance standards. This contribution is significant in enhancing the understanding of each framework's role in cybersecurity, advocating for a cohesive approach to compliance and risk management.

VII. FUTURE WORK

Future research should refine criteria and explore new frameworks to keep pace with the dynamic cybersecurity

TABLE III
MAPPING OF SCF DOMAINS WITH SEVEN MAJOR COMPLIANCES

#	SCF Domain	SOC 2 (TSC)	GDPR	PCI DSS	HIPAA	CIS Controls V8	NIST CSF	CMMC
1	Cybersecurity & Data Privacy Governance	✓	✓	✓	✓		✓	
2	Artificial and Autonomous Technology							
3	Asset Management	✓	✓	✓	✓	✓	✓	✓
4	Business Continuity & Disaster Recovery	✓	✓	✓	✓	✓	✓	✓
5	Capacity & Performance Planning	✓	✓				✓	
6	Change Management	✓	✓	✓			✓	✓
7	Cloud Security		✓	✓				✓
8	Compliance	✓	✓	✓	✓		✓	✓
9	Configuration Management	✓	✓	✓		✓	✓	✓
10	Continuous Monitoring	✓	✓	✓	✓	✓	✓	✓
11	Cryptographic Protections	✓	✓	✓	✓	✓	✓	✓
12	Data Classification & Handling	✓	✓	✓	✓	✓	✓	✓
13	Embedded Technology		✓					
14	Endpoint Security	✓	✓	✓	✓	✓	✓	✓
15	Human Resources Security	✓	✓	✓	✓	✓	✓	✓
16	Identification & Authentication	✓	✓	✓	✓	✓	✓	✓
17	Incident Response	✓	✓	✓	✓	✓	✓	✓
18	Information Assurance	✓	✓	✓	✓	✓		✓
19	Maintenance		✓	✓	✓	✓	✓	✓
20	Mobile Device Management	✓						✓
21	Network Security	✓	✓	✓		✓	✓	✓
22	Physical & Environmental Security	✓	✓	✓	✓		✓	✓
23	Data Privacy	✓	✓	✓	✓	✓		
24	Project & Resource Management	✓	✓	✓		✓	✓	
25	Risk Management	✓	✓	✓	✓	✓	✓	✓
26	Secure Engineering & Architecture	✓	✓	✓	✓	✓	✓	✓
27	Security Operations	✓	✓	✓				✓
28	Security Awareness & Training	✓	✓	✓	✓	✓	✓	✓
29	Technology Development & Acquisition	✓	✓	✓		✓	✓	✓
30	Third-Party Management	✓	✓	✓	✓	✓	✓	
31	Threat Management	✓	✓	✓			✓	✓
32	Vulnerability & Patch Management	✓	✓	✓		✓	✓	✓
33	Web Security		✓	✓		✓		

field. Additionally, we aim to further investigate the Unified Compliance Map's practical use with the SCF, focusing on case studies to showcase our framework's effectiveness in meeting multiple standards at once.

ACKNOWLEDGMENT

This material is based in part upon work supported by the National Science Foundation under Grant No. MRI20 CNS-2018611.

REFERENCES

[1] ETSI, "Global Cyber Security Ecosystem," ETSI TR 103 306 V1.2.1, Jul. 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.02.01_60/tr_103306v010201p.pdf. [Accessed: Jul. 31, 2023].

[2] T. Poppensieker and R. Riemenschnitter, "A new posture for cybersecurity in a networked world," Mckinsey.com, 09-Mar-2018. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world/. [Accessed: 12-Sep-2023].

[3] "Internet Organised Crime Assessment (IOCTA) 2023," Europol. [Online]. Available: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023. [Accessed: 9-Sep-2023].

[4] "Top 7 cyber security trends in 2023," Check Point Software, 07-Sep-2023. [Online]. Available: https://www.checkpoint.com/cyber-hub/cyber-security/top-7-cyber-security-trends-in-2023/. [Accessed: 21-Sep-2023].

[5] "What is GRC (Governance, Risk, and Compliance)?," OCEG. [Online]. Available: https://www.oceg.org/ideas/what-is-grc/. [Accessed: 27-Sep-2023].

[6] A. Papazafeiropoulou and K. Spanaki, "Understanding governance, risk and compliance information systems (GRC IS): The experts view," Inf. Syst. Front., vol. 18, no. 6, pp. 1251–1263, 2016.

[7] PricewaterhouseCoopers, "Driven performance: A new strategy for success through integrated governance, risk and compliance management," Frankfurt: PricewaterhouseCoopers International Limited, 2004. [White paper].

[8] S. Gill and U. Purushottam, "Integrated GRC-is your organization ready to move," Governance, risk and compliance, SETLabs Briefings, pp. 37-46, 2008.

[9] N. Racz, E. Weippl, and A. Seufert, "A process model for integrated IT governance, risk, and compliance management," in Proc. Ninth Int. Baltic Conf. on Databases and Information Systems (Baltic DB&IS 2010), J. Barzdins and M. Kirikova, Eds. Riga: University of Latvia Press, 2010, pp. 155-170.

[10] B. Marr, "The 10 biggest cyber security trends in 2024 everyone must be ready for now," Forbes, 11-Oct-2023. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/?sh=59a87f695f13. [Accessed: 21-Oct-2023].

[11] R. Foorthuis, "Tactics for internal compliance: A literature review," arXiv [cs.CY], 2020.

[12] T. Tam, A. Rao, and J. Hall, "The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses," Comput. Secur., vol. 109, no. 102385, p. 102385, 2021.

[13] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Rep., vol. 7, pp. 8176-8186, 2021.

[14] M. Mubarkoot, J. Altmann, M. Rasti-Barzoki, B. Egger, and H. Lee, "Software compliance requirements, factors, and policies: A systematic

literature review," Comput. Secur., vol. 124, no. 102985, p. 102985, 2023.
[15] M. Hashmi, G. Governatori, H.-P. Lam, and M. T. Wynn, "Are we done with business process compliance: state of the art and challenges ahead," Knowl. Inf. Syst., vol. 57, no. 1, pp. 79–133, 2018.
[16] R. A. Nafea and M. Amin Almaiah, "Cyber Security Threats in Cloud: Literature Review," in 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 779-786, doi: 10.1109/ICIT52682.2021.9491638.
[17] D. Yimam and E. B. Fernandez, "A survey of compliance issues in cloud computing," J. Internet Serv. Appl., vol. 7, no. 1, 2016.
[18] N. Ameen, A. Tarhini, M. H. Shah, N. Madichie, J. Paul, and J. Choudrie, "Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce," Comput. Human Behav., vol. 114, no. 106531, p. 106531, 2021.
[19] O. Klymenko, S. Meisenbacher, and F. Matthes, "Identifying practical challenges in the implementation of technical measures for data privacy compliance," arXiv [cs.CR], 2023.
[20] J. Ruiter and M. Warnier, "Privacy regulations for cloud computing: Compliance and implementation in theory and practice," in Computers, Privacy and Data Protection: an Element of Choice, Dordrecht: Springer Netherlands, 2011, pp. 361–376.
[21] K. W. Ullah, A. S. Ahmed and J. Ylitalo, "Towards Building an Automated Security Compliance Tool for the Cloud," 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, 2013, pp. 1587-1593, doi: 10.1109/TrustCom.2013.195.
[22] M. Daud, et al., "Bridging the gap between organisational practices and cyber security compliance: can cooperation promote compliance in organisations?," Int. J. Bus. Soc., vol. 19, no. 1, 2018.
[23] M. Harris and S. Furnell, "Routes to security compliance: be good or be shamed?," Comput. Fraud Secur., vol. 2012, no. 12, pp. 12–20, 2012.
[24] R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance," Appl. Sci. (Basel), vol. 11, no. 8, p. 3383, 2021.
[25] A. Alahmari and B. Duncan, "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2020, pp. 1-5, doi: 10.1109/CyberSA49311.2020.9139638.
[26] A. Chidukwani, S. Zander and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," IEEE Access, vol. 10, pp. 85701-85719, 2022, doi: 10.1109/ACCESS.2022.3197899.
[27] M. Alotaibi, S. Furnell and N. Clarke, "Information security policies: A review of challenges and influencing factors," 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 2016, pp. 352-358, doi: 10.1109/ICITST.2016.7856729.
[28] P. Balozian and D. Leidner, "Review of IS security policy compliance: Toward the building blocks of an IS security theory," SIGMIS Database, vol. 48, no. 3, pp. 11–43, 2017.
[29] S. Highlights, "The global state of information security® survey 2018," Pwc.com. [Online]. Available: https://www.pwc.com/sg/en/publications/assets/gsiss-2018.pdf. [Accessed: 11-Dec-2023].
[30] M. Usman, M. Felderer, M. Unterkalmsteiner, E. Klotins, D. Mendez, and E. Alégroth, "Compliance requirements in large-scale software development: An industrial case study," in Product-Focused Software Process Improvement, Cham: Springer International Publishing, 2020, pp. 385–401.
[31] O. Akhigbe, D. Amyot, and G. Richards, "A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance," Requir. Eng., vol. 24, no. 4, pp. 459–481, 2019.
[32] Amazon Web Services, "Quick Starts," Amazon Web Services. [Online]. Available: https://aws.amazon.com/quickstart/. [22-Oct-2023].
[33] Amazon Web Services, "PCI DSS and AWS Foundational Security Best Practices on AWS ," Amazon Web Services. [Online]. Available: https://aws.amazon.com/solutions/implementations/compliance-pci-fsbp-remediation/. [22-Oct-2023].
[34] Amazon Web Services, "HIPAA Reference Architecture on AWS," Amazon Web Services. [Online]. Available: https://aws.amazon.com/solutions/implementations/compliance-hipaa/. [22-Oct-2023].
[35] Rapid7, "Solutions for GRC," Rapid7, [Online]. Available: https://www.rapid7.com/solutions/. [Accessed: 1-Sep-2023]
[36] "Word crimes part 1 – taking on compliance: Statutory vs regulatory vs contractual compliance," Tripwire.com. [Online]. Available: https://www.tripwire.com/state-of-security/statutory-vs-regulatory-vs-contractual-compliance. [Accessed: 14-Sep-2023].
[37] American Institute of Certified Public Accountants (AICPA), "Service Organization Control 2 (SOC 2)," [Online]. Available: https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022. [Accessed: 20-Aug-2023].
[38] European Parliament and Council of the European Union, "General Data Protection Regulation," Official Journal of the European Union, L119, pp. 1-88, 2016.
[39] Payment Card Industry Security Standards Council, "Payment Card Industry Data Security Standard (PCI DSS) Version 4.0," [Online]. Available: [https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf]. [Accessed: 1-Sep-2023].
[40] U.S. Department of Health and Human Services, "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," [Online]. Available: [https://www.hhs.gov/hipaa/index.html]. [Accessed: 10-Aug-2023].
[41] HIPAA Journal, "What are the Penalties for HIPAA Violations?," HIPAA Journal, 2024. [Online]. Available: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/. [Accessed: 10-Dec-2023].
[42] Center for Internet Security, "CIS Controls V8," [Online]. Available: [https://www.cisecurity.org/controls/v8]. [Accessed: 10-Sep-2023].
[43] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)," Version 1.1, 2018, [Online]. Available: [https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf]. [Accessed: 2-Sep-2023].
[44] A. Mahn, J. Marron, S. Quinn, and D. Topper, "Getting started with the NIST Cybersecurity Framework: A quick start guide," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, 2021.
[45] U.S. Department of Defense, "Cybersecurity Maturity Model Certification (CMMC) 2.0," 2021, [Online]. Available: [https://dodcio.defense.gov/CMMC/Model/]. [Accessed: 3-Sep-2023].
[46] U.S. Department of Defense, "Cybersecurity Maturity Model Certification (CMMC) Model Overview," 2021, [Online]. Available: [https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf]. [Accessed: 3-Sep-2023].
[47] O. Giuca, T. M. Popescu, A. M. Popescu, G. Prostean, and D. E. Popescu, "A survey of cybersecurity risk management frameworks," in Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), Vol. I 8, Springer International Publishing, 2021, pp. 240-272.
[48] The Open Group, "The Open Group Risk Taxonomy (O-RT) Standard, Version 3.0.1," Opengroup.org. [Online]. Available: https://pubs.opengroup.org/security/o-rt/. [Accessed: 23-Nov-2023].
[49] SCF Council, "Secure Controls Framework," Securecontrolsframework.com. [Online]. Available: https://securecontrolsframework.com/. [Accessed: 27-Sep-2023].
[50] SCF Council, "Secure Controls Framework (SCF) Overview & Instructions," Securecontrolsframework.com [Online]. Available: https://content.securecontrolsframework.com/SCF-Recommended-Practices.pdf. [Accessed: 28-Sep-2023].
[51] SCF Community, "Secure Controls Framework (SCF) download," Securecontrolsframework.com. [Online]. Available: https://securecontrolsframework.com/scf-download/. [Accessed: 14-Dec-2023].
[52] W. Wang, "SCFMapping," GitHub repository, [Online]. Available: https://github.com/Wenjia1215/SCFMapping. [Accessed: 1-Dec-2023].