IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

A Guide to become NIST Compliant

Zahra Sayed[1], Durriya Bandukwala[2], Ayaaz Idrisi[3], Aarish Faki[4], Er. Asadullah Shaikh[5], Sharique Shaikh[6], Najib Baig Mirza[7]
Students, Department of Computer Engineering[1,2,3,4]
Professor, Department of Computer Engineering[5]
Founders, CNCM LLC[6,7]
M.H. Saboo Siddik College of Engineering, Mumbai, Maharashtra, India[1,2,3,4,5]

Abstract: *The National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other tools to meet the needs of American business, government organizations, and the general public. Their work spans from giving businesses accurate information that they can utilize immediately to longer-term research that anticipates technology developments and future challenges. Moreover, the needs of American industry and the general public are what drive their cybersecurity endeavors. They collaborate closely with stakeholders to set priorities and ensure that our resources are focused on the most urgent issues they face. NIST also advances the management of privacy risks, some of which are directly connected to cybersecurity, and broadens our understanding of those risks. Among the main areas on which NIST contributes and focuses are cryptography, education and workforce, emerging technologies, risk management, identity and access management, measurements, privacy, trustworthy networks, and trustworthy platforms. This research paper aims to focus on discussing the various controls of the NIST. It also emphasizes on the processes to be followed by the federal agencies to ensure that they are NIST compliant.*

Keywords: Compliance, NIST 800-53, Automation, Cyber Security

I. INTRODUCTION

All U.S. federal information systems, with the exception of those pertaining to national security, are covered by a list of security and privacy measures in NIST Special Publication 800-53. It is issued by the United States Department of Commerce's non-regulatory National Institute of Standards and Technology. In order to help federal agencies implement the Federal Information Security Modernization Act of 2014 (FISMA) and manage cost-effective programs to safeguard their information and information systems, NIST develops and publishes standards, recommendations, and other publications. The 800-53A and 800-53B publications, which offer guidelines and baselines based on 800-53, are two linked documents.

So what does NIST compliant mean? NIST compliance depends on which NIST framework is being used. We will focus on NIST 800-53, used for risk management

1..1 NIST 800-53

The Federal Information Processing Standard's (FIPS) minimum baseline for security measures is defined by NIST 800-53. It lists more than 1,000 controls and 20 different control families, such as incident response, risk assessment, and access control.

This list of security measures enables federal government agencies to implement the privacy and security measures that are suggested for federal information systems and organizations to safeguard against security threats and cyberattacks. In this paper, we'll examine the 18 NIST 800 53 control families and provide a summary of the NIST standards list.

B. NIST 800-53A- Assessing Security and Privacy Controls in Information Systems and Organizations

An in-depth examination of NIST 800-53A will help you comprehend the criteria of NIST 800-53 since it is an extension and offers further instructions on how to perform assessments of these controls. It is easier to grasp because of the additional instructions on these controls

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

C. NIST 800-53B- Control Baselines for Information Systems and Organizations

A relatively recent standard, NIST 800-53B, provides security and privacy baselines for government information systems and organizations. Thus, the control baselines from 800-53 have been transferred to this new standard. Again, the system owner chooses which of the three baselines—Low, Medium, and High—to use.

II. NIST 800-53 CONTROL FAMILIES

2.1 AC - Access Control

The security specifications for the AC Control Family provide system logging. When determining when users may access the system and their amount of access, this covers account management, system rights, and remote access tracking. It also includes who has access to what assets.

2.2 AU - Audit and Accountability

Security controls pertaining to an organization's audit capabilities are included in the AU control family. This covers audit guidelines and practices, audit recording, creation of audit reports, and safeguarding of audit data..

2.3 AT - Awareness and Training

The AT Control Family's control sets are unique to your security policies, practices, and training records.

2.4 CM - Configuration Management

The configuration management policies of an organization determine the CM controls. This provides a base configuration that will serve as the foundation for further information system builds and modifications. This comprises security impact analysis controls and inventories of the components of information systems.

2.5 CP - Contingency Planning

The CP control family provides controls particular to a company's backup plan in the case of a cybersecurity incident. This includes safeguards including testing, upgrading, training, backups, and system reconstitution for contingency plans.

2.6 IA - Identification and Authentication

IA controls are specific to identification and authentication processes inside an organization. This encompasses both the management of such systems and the identification and authentication of users inside and outside of organizations.

2.7 MP - Media Protection

The controlling family for media protection includes measures for access, marking, storage, transit regulations, sanitization, and specified organizational media usage.

2.8 PS - Personnel Security

PS controls refer to the methods a business uses to safeguard its employees, including access agreements, personnel screening, termination, and position risk.

2.9 PE - Physical and Environmental Protection

To defend against physical dangers, the Physical and Environmental Protection control family is installed on systems, buildings, and supporting infrastructure. Physical access authorizations, surveillance, visitor logs, emergency shutoffs, electricity, lighting, fire prevention, and water damage protection are a few of these controls.

2.10 PL - Planning

The objective, scope, roles, duties, management commitment, coordination among entities, and organizational compliance are all addressed in the NIST SP 800-53 control PL family, which is particular to an organization's security planning policies.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

2.11 PM - Program Management

The PM control family is particular to who oversees and controls your cybersecurity program. A critical infrastructure plan, information security program plan, plan of action milestones and processes, risk management strategy, and enterprise architecture are just a few examples of what is covered.

2.12 RA - Risk Assessment

The RA control family pertains to a company's vulnerability scanning tools and risk assessment procedures.

2.13 CA - Security Assessment and Authorization

Controls that support the execution of security assessments, authorizations, continuous monitoring, plans of action and milestones, and system interconnections are included in the Security Assessment and Authorization control family.

2.14 SC - System and Communications Protection

Procedures for protecting systems and communications are under the authority of the SC control family. Boundary protection, information at rest protection, collaborative computing devices, cryptographic protection, denial of service protection, and many other types are included in this.

2.15 SI - System and Information Integrity

The family of SI controls correspond to those that safeguard data and system integrity. NIST SI 7, which addresses fault rectification, malicious code protection, information system monitoring, security warnings, software, firmware integrity, and spam protection, is a member of this control family.

2.16 SA - System and Services Acquisition

The SA control family is related to controls that safeguard allotted resources and the system development life cycle of an organization. This comprises developer security testing and assessment controls, development configuration management controls, and controls over information system documentation.

The cybersecurity operations of a company may be streamlined and coordinated across many standards and guidelines with the aid of an integrated cyber risk management system like CyberStrong, saving teams time, effort, and resources while maintaining compliance.

2.17 SR- Supply chain Risk Management

Controls for supply chain risk management set up procedures to reduce supply chain hazards. It covers supplier management, supplier evaluations, and supply chain component inspections.

2.18 PT- Personally Identifiable Information Processing and Transparency

Sensitive data are protected by processing and transparency rules for personally identifiable information (PII). This control family emphasizes user data protection and permission. Having the appropriate rules in place to preserve and manage all PII aids firms in reducing the risks related to data branches.

III. METHODOLOGY

The United States Department of Commerce's non-regulatory National Institute of Standards and Technology (NIST) creates and disseminates standards, guidelines, and best practices for a variety of subjects, including information technology, data protection, and cybersecurity. Companies generally adhere to the guidelines and suggestions offered by NIST in their publications to be NIST compliant.

Following are a few typical actions businesses take to comply with NIST:

1. Risk assessments are carried out by businesses to determine possible threats and weaknesses to their systems and data. This entails assessing the probability and consequences of various scenarios and developing mitigation plans for those risks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

2. Implementing security controls: Organizations put the NIST-recommended security measures, such as access controls, encryption, and tracking, into practice. These safeguards aid in preventing unauthorized entry, data breaches, and other security calamities.
3. Creating policies and procedures: Businesses create policies and procedures to instruct staff members on how to handle confidential data, report security incidents, and adhere to legal requirements.
4. Employee education: Businesses educate their staff members to ensure they know the organization's security policies and practices.

IV. TOOLS TO AUTOMATE COMPLIANCE

4.1 Drata

Drata is a cloud-based security and compliance automation platform that can help organizations automate NIST 800-53 compliance. Here are some ways that Drata can help:

1. Control Mapping: Drata can automatically map your existing controls to the NIST 800-53 control framework. This allows you to identify gaps in your current control environment and ensure that you have the necessary controls in place to meet the NIST 800-53 requirements.
2. Automated Assessment: Drata can automate the assessment process for NIST 800-53 compliance. The platform uses machine learning algorithms to collect and analyze data from various sources, including vulnerability scans, security logs, and configuration files, to identify potential security risks and vulnerabilities.
3. Continuous Monitoring: Drata provides continuous monitoring of your IT infrastructure to ensure ongoing compliance with NIST 800-53. The platform can automatically generate reports and alerts when there are changes to your control environment, such as new vulnerabilities or changes to your IT infrastructure.
4. Compliance Reporting: Drata can generate compliance reports that demonstrate your organization's compliance with NIST 800-53. These reports can be customized to meet your specific compliance needs and can be shared with auditors and other stakeholders.

4.2 CyberSaint

CyberSaint is a comprehensive risk management system that aids in the automation and simplification of NIST 800-53 compliance efforts. It is intended to assist businesses in more efficiently and successfully managing their risk management and compliance procedures.

By bringing together multiple data sources, such as threat intelligence feeds, vulnerability evaluations, and compliance guidelines, CyberSaint's platform provides a centralized perspective of an organization's risk position and compliance state. CyberSaint can provide a complete view of an organization's risk and compliance stance by combining these sources, enabling them to spot possible holes and take remedial actions.

One of CyberSaint's main benefits is its ability to automate the compliance process. The platform includes processes and templates that enable companies to map their current controls to the NIST 800-53 framework swiftly and simply. CyberSaint also gives real-time feedback on control effectiveness and highlights places where controls may need to be improved.

The reporting powers of CyberSaint also assist companies in demonstrating compliance to inspectors and authorities. The tool includes customizable dashboards and reports to help companies measure and evaluate their compliance efforts.

Overall, CyberSaint is a good option for businesses that want to simplify and manage their NIST 800-53 compliance efforts. CyberSaint can help organizations improve their overall security posture and reduce their risk of data breaches and other security events by giving a complete picture of an organization's risk posture and automating the compliance process.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

4.3 HIPAA One

HIPAA One is a software solution designed to assist healthcare organizations in complying with the Health Insurance Portability and Accountability Act (HIPAA). HIPAA One offers a suite of tools that help healthcare providers, business associates, and covered entities perform a risk analysis and assess their overall compliance with HIPAA regulations.

The software helps organizations identify potential vulnerabilities in their data security practices, policies, and procedures. HIPAA One also provides recommendations for addressing any identified issues and generates reports that can be used to demonstrate compliance with HIPAA regulations to auditors, regulators, and other stakeholders.

HIPAA One is a popular choice for healthcare organizations seeking to simplify and streamline their compliance efforts, reduce the risk of data breaches, and avoid costly penalties for noncompliance.

Here is a detailed explanation of how HIPAA One works:

- **Assessment:** The assessment step in HIPAA One involves a series of questions that are used to evaluate a healthcare organization's compliance with the HIPAA Security Rule. The questions cover a wide range of topics related to administrative, physical, and technical safeguards, such as access controls, disaster recovery, incident response, and data encryption. During the assessment step, the user is prompted to answer these questions and provide additional information as needed. Based on the user's answers, the software generates a risk assessment report that identifies potential vulnerabilities in the organization's security measures, policies, and procedures. The assessment step is crucial because it provides a starting point for the compliance process. By answering the assessment questions, the user can identify areas where the organization is at risk of non-compliance and take action to address any issues. The risk assessment report generated by the software is used as a baseline to evaluate the effectiveness of any corrective actions taken and to monitor ongoing compliance with HIPAA regulations. In summary, the assessment step in HIPAA One is a critical first step in the compliance process. It involves a series of questions that help identify potential vulnerabilities in the organization's security measures, policies, and procedures. The risk assessment report generated by the software provides a baseline for compliance and helps healthcare organizations take action to address any issues and maintain ongoing compliance with HIPAA regulations.
- **Identification of Vulnerabilities:** The identification of vulnerabilities in HIPAA One is a critical step in the compliance process for healthcare organizations. During this step, the software analyzes the risk assessment report generated in the assessment step to identify potential weaknesses in the organization's security measures, policies, and procedures. The software considers various factors such as the organization's assets, threats, and likelihood of occurrence to determine the severity of each vulnerability. Once the vulnerabilities are identified, the software generates a vulnerability summary that outlines the potential risks to the organization and the severity of each vulnerability. This information is used to prioritize the vulnerabilities and determine which ones require immediate attention. The identification of vulnerabilities is essential because it helps healthcare organizations understand their security risks and take action to address any issues. By prioritizing the vulnerabilities, organizations can focus their resources on the most critical areas and implement the necessary security controls to mitigate the risks.
- **Risk analysis:** It is an essential step in HIPAA compliance that aims to evaluate potential vulnerabilities and threats to an organization's protected health information (PHI). The process involves identifying and assessing risks to PHI, prioritizing areas of concern, and developing a plan to mitigate the identified risks. The risk analysis process involves four primary steps, including identifying PHI, documenting potential threats to PHI, evaluating current security measures, and determining the likelihood and impact of identified risks. To begin, the organization must identify all PHI within its system, including electronic and paper records, and any other data containing PHI. Then, it must identify and document all potential threats to PHI in detail, whether from external sources or internal sources. After identifying threats, the organization must evaluate its existing security measures, including physical, administrative, and technical safeguards, in place to protect PHI. This evaluation should consider all potential threats identified in the previous step. Finally, the organization must determine the likelihood and potential impact of each identified risk. By prioritizing risks based on their likelihood of occurrence and potential impact, the organization can develop a plan to mitigate the risks and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

maintain compliance with HIPAA regulations.In summary, risk analysis is a critical process that enables healthcare organizations to identify and assess vulnerabilities and threats to PHI. By evaluating potential risks and current security measures, organizations can develop a plan to mitigate risks and comply with HIPAA regulations.

- **Recommendations:** Recommendations play a vital role in HIPAA compliance, which helps healthcare organizations manage vulnerabilities and risks effectively. These recommendations are based on the results of the risk analysis and vulnerability identification process, which highlights the areas that require improvement. The recommendations given by HIPAA One are prioritized based on the severity of the identified vulnerabilities. The most critical ones are given the highest priority to ensure that the healthcare organization takes swift action to address them. Recommendations are grouped into three categories: administrative, physical, and technical controls. Administrative recommendations focus on training, policies, and procedures to ensure that the healthcare organization complies with HIPAA regulations. Physical recommendations center around the security of facilities and equipment, while technical recommendations deal with technical safeguards and controls to protect PHI. Following the recommendations given by HIPAA One helps healthcare organizations to comply with HIPAA regulations, maintain PHI confidentiality, integrity, and availability, and safeguard patient privacy. By adhering to these guidelines, healthcare organizations can improve their security posture, identify and address vulnerabilities, and reduce the likelihood of a data breach.
- **Compliance reporting:** Compliance reporting is an essential component of HIPAA compliance, which involves generating reports that demonstrate the organization's compliance with HIPAA regulations. Compliance reporting is necessary to identify gaps in the organization's security posture and to document the measures that have been taken to address those gaps. This documentation can be used to demonstrate to auditors that the organization is in compliance with HIPAA regulations. The compliance reporting process begins by reviewing the organization's policies, procedures, and security measures to ensure that they meet HIPAA standards. Once the review is complete, the organization can generate reports that demonstrate their compliance with HIPAA regulations. Compliance reporting can take several forms, including self-audits, third-party audits, and risk analysis reports. Self-audits involve the organization reviewing its policies and procedures to ensure that they meet HIPAA standards. Third-party audits are conducted by external auditors who review the organization's security measures and policies to ensure that they meet HIPAA regulations. Risk analysis reports are generated as a result of the risk analysis process and document the organization's vulnerabilities and risks. Compliance reporting can also include documentation of security incidents and breaches, as well as any corrective actions that have been taken to address those incidents. This documentation can be used to demonstrate to auditors that the organization is taking steps to address security incidents and prevent future breaches. Compliance reporting is an ongoing process that requires regular review and monitoring to ensure that the organization remains in compliance with HIPAA regulations. By regularly generating compliance reports, healthcare organizations can identify and address gaps in their security measures and policies, reduce the likelihood of a data breach, and protect the confidentiality, integrity, and availability of PHI.

4.4 HyperProof

Hyperproof is a software application designed to streamline the process of proof creation and management for compliance professionals, auditors, and legal teams. The platform provides a centralized hub for organizing and tracking evidence, documenting compliance workflows, and generating reports to demonstrate regulatory compliance.

Hyperproof uses a combination of advanced technology and user-friendly interfaces to automate many of the tasks involved in compliance management. The platform can integrate with various systems, including cloud storage, SaaS applications, and file-sharing platforms, to collect and collate evidence in one place.

Hyperproof also includes a range of features to help users stay on top of compliance requirements, such as customizable workflows, document templates, and automated alerts for deadlines and expirations. The platform's reporting and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

analytics tools allow users to generate detailed reports that provide insights into their organization's compliance posture and identify areas for improvement.

Overall, Hyperproof aims to simplify the complex process of compliance management by providing a centralized, automated platform that makes it easier for teams to stay on top of regulatory requirements and maintain a robust compliance posture.

The specific steps involved in using Hyperproof can vary depending on the user's needs and goals, but here is an overview of some of the key steps typically involved:

1. **Define compliance requirements:** The first step is to identify the relevant regulatory requirements, industry standards, and internal policies that apply to your organization. This information is used to create a compliance framework within Hyperproof.
2. **Collect and organize evidence:** Hyperproof allows you to collect evidence from various sources, such as cloud storage platforms or software applications, and organize it in one place. This evidence can include documents, contracts, policies, and other types of records that demonstrate compliance.
3. **Create workflows:** Hyperproof allows you to create customizable workflows that map out the compliance process and assign tasks to different team members. This helps ensure that everyone is working together efficiently and that deadlines are met.
4. **Monitor and manage compliance:** Hyperproof includes features that allow you to monitor your compliance status in real-time, track progress towards compliance goals, and generate alerts for upcoming deadlines or expirations.
5. **Generate reports:** Hyperproof provides a range of reporting and analytics tools that enable you to generate reports on your compliance status and performance. These reports can be used to demonstrate compliance to regulators, auditors, or other stakeholders.
6. **Continuously improve:** Finally, Hyperproof allows you to continuously improve your compliance posture by identifying areas for improvement and implementing corrective actions. This helps ensure that your organization stays compliant and reduces the risk of regulatory violations or legal penalties.

V. ARCHITECTURE

The four cybersecurity platforms, HIPAA One, Drata, Hyperproof, and CyberSaint Security, all have similar layers in their architectural models because they all follow best practices for designing secure and scalable systems. These layers are commonly found in many different types of software systems and provide a framework for organizing and structuring the various components of the system.

Additionally, all four platforms are focused on helping organizations manage cybersecurity risk and compliance, so their architectures are designed to support these goals. This includes having a user interface layer that is easy to use and understand, an application layer that provides the necessary tools and features to manage risk and compliance, and a data layer that securely stores and manages compliance data.

However, each platform may have unique features or components that are specific to their intended use cases or target markets. As a result, while the basic layers of the architectural models may be similar, there may be differences in how these layers are implemented or the specific components that are included in each layer.

5.1 HIPAA One

HIPAA One is a comprehensive compliance solution designed to help healthcare organizations and their business associates comply with the regulations outlined in the Health Insurance Portability and Accountability Act (HIPAA). The platform operates on a cloud-based SaaS model, which means that it is hosted on secure servers and accessible to users over the internet.

The architecture of the HIPAA One platform is designed to be scalable, flexible, and customizable, making it suitable for organizations of all sizes. The platform is built on modern technologies that allow it to integrate with other healthcare systems, applications, and tools, enabling seamless data sharing and collaboration.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

One of the key benefits of the cloud-based architecture of HIPAA One is its accessibility. The platform can be accessed from anywhere, at any time, by authorized users. This means that healthcare organizations can manage their compliance program remotely, without the need for physical infrastructure or on-site IT support.

The platform is also designed to be secure, with robust encryption and authentication mechanisms in place to protect sensitive data. The servers hosting the platform are maintained by the vendor, who is responsible for ensuring that they are up-to-date and secure at all times. The platform also includes features such as automatic updates, data backup, and disaster recovery, ensuring that organizations can maintain compliance even in the event of a system failure or outage.

Another key feature of the HIPAA One platform is its flexibility. The platform is customizable, allowing organizations to tailor it to their specific needs and requirements. This includes the ability to customize risk assessments, policy templates, and compliance tracking features, enabling organizations to create a compliance program that works best for them.

HIPAA One can be conceptualized as having several layers, each of which plays a vital role in ensuring that the platform operates effectively and securely. The following are the layers of the HIPAA One architecture:

- **User Interface Layer:** The user interface layer is the layer that allows users to interact with the HIPAA One platform. It includes the web application and mobile app interfaces that allow users to log in, view compliance data, and interact with the various tools and features of the platform. The user interface layer is designed to be user-friendly and intuitive, enabling users to navigate the platform easily and efficiently.
- **Application Layer:** The application layer is the layer that manages the business logic and functionality of the HIPAA One platform. This layer includes the tools and features that enable healthcare organizations to manage their compliance program effectively. For example, the risk assessment tool enables organizations to identify potential security risks, while the policy management tool enables organizations to create, manage, and enforce policies and procedures related to HIPAA compliance.
- **Data Layer:** The data layer is the layer that stores and manages the data generated by the HIPAA One platform. This includes compliance data, such as risk assessments, policies, and audit logs, as well as user data, such as login credentials and access permissions. The data layer is designed to be secure and scalable, with robust data backup and recovery mechanisms in place to ensure that data is always available when needed.
- **Integration Layer:** The integration layer is the layer that enables HIPAA One to integrate with other healthcare systems, applications, and tools. This layer includes APIs and other integration mechanisms that allow data to be exchanged between HIPAA One and other systems, enabling seamless data sharing and collaboration. For example, HIPAA One can integrate with electronic health record (EHR) systems, allowing healthcare providers to access compliance data directly from their EHR.
- **Infrastructure Layer:** The infrastructure layer is the layer that provides the underlying computing resources needed to run the HIPAA One platform. This includes physical servers, networking equipment, and other infrastructure components needed to host the platform and ensure its availability and reliability. The infrastructure layer is designed to be scalable and resilient, with multiple redundancies and failover mechanisms in place to ensure that the platform is always available when needed.

5.2 Drata

Drata is a cloud-based compliance automation platform that helps businesses achieve and maintain SOC 2 compliance. The Drata platform is built using a multi-tiered architecture that includes the following layers:

1. **User Interface Layer:** The user interface layer is the topmost layer of the Drata architecture. This layer includes the web application and mobile app interfaces that allow users to log in, view compliance data, and interact with the various tools and features of the platform. The user interface layer is designed to be user-friendly and intuitive, enabling users to navigate the platform easily and efficiently.
2. **Application Layer:** The application layer is the layer that manages the business logic and functionality of the Drata platform. This layer includes the tools and features that enable businesses to manage their compliance program effectively. For example, the risk assessment tool enables businesses to identify potential security

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

risks, while the policy management tool enables businesses to create, manage, and enforce policies and procedures related to SOC 2 compliance.

3. **Data Layer:** The data layer is the layer that stores and manages the data generated by the Drata platform. This includes compliance data, such as risk assessments, policies, and audit logs, as well as user data, such as login credentials and access permissions. The data layer is designed to be secure and scalable, with robust data backup and recovery mechanisms in place to ensure that data is always available when needed.
4. **Integration Layer:** The integration layer is the layer that enables Drata to integrate with other systems, applications, and tools. This layer includes APIs and other integration mechanisms that allow data to be exchanged between Drata and other systems, enabling seamless data sharing and collaboration. For example, Drata can integrate with cloud infrastructure providers, allowing businesses to assess the compliance of their cloud environments.
5. **Infrastructure Layer:** The infrastructure layer is the layer that provides the underlying computing resources needed to run the Drata platform. This includes physical servers, networking equipment, and other infrastructure components needed to host the platform and ensure its availability and reliability. The infrastructure layer is designed to be scalable and resilient, with multiple redundancies and failover mechanisms in place to ensure that the platform is always available when needed.

In summary, the layers of the Drata architecture work together to provide a comprehensive compliance solution that is secure, scalable, and customizable. The user interface layer enables users to interact with the platform easily, while the application layer provides the tools and features needed to manage a SOC 2 compliance program effectively. The data layer stores and manages compliance data securely, while the integration layer enables seamless data sharing and collaboration. Finally, the infrastructure layer provides the underlying computing resources needed to run the platform and ensure its availability and reliability.

5.3 CyberSaint

CyberSaint Security is a cybersecurity and compliance automation platform that helps organizations manage their cybersecurity risk and compliance programs. The CyberSaint Security platform is built on a multi-layered architecture that includes the following layers:

1. **User Interface Layer:** The user interface layer is the topmost layer of the CyberSaint Security architecture. This layer includes the web application interface that allows users to log in, view compliance data, and interact with the various tools and features of the platform. The user interface layer is designed to be user-friendly and intuitive, enabling users to navigate the platform easily and efficiently.
2. **Application Layer:** The application layer is the layer that manages the business logic and functionality of the CyberSaint Security platform. This layer includes the tools and features that enable organizations to manage their cybersecurity and compliance programs effectively. For example, the risk assessment tool enables organizations to identify potential security risks, while the policy management tool enables organizations to create, manage, and enforce policies and procedures related to cybersecurity and compliance.
3. **Data Layer:** The data layer is the layer that stores and manages the data generated by the CyberSaint Security platform. This includes compliance data, such as risk assessments, policies, and audit logs, as well as user data, such as login credentials and access permissions. The data layer is designed to be secure and scalable, with robust data backup and recovery mechanisms in place to ensure that data is always available when needed.
4. **Integration Layer:** The integration layer is the layer that enables CyberSaint Security to integrate with other systems, applications, and tools. This layer includes APIs and other integration mechanisms that allow data to be exchanged between CyberSaint Security and other systems, enabling seamless data sharing and collaboration. For example, CyberSaint Security can integrate with other security tools, such as vulnerability scanners and SIEM systems, to provide a more comprehensive view of an organization's cybersecurity posture.
5. **Infrastructure Layer:** The infrastructure layer is the layer that provides the underlying computing resources needed to run the CyberSaint Security platform. This includes physical servers, networking equipment, and other infrastructure components needed to host the platform and ensure its availability and reliability. The

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

infrastructure layer is designed to be scalable and resilient, with multiple redundancies and failover mechanisms in place to ensure that the platform is always available when needed.

In summary, the layers of the CyberSaint Security architecture work together to provide a comprehensive cybersecurity and compliance solution that is secure, scalable, and customizable. The user interface layer enables users to interact with the platform easily, while the application layer provides the tools and features needed to manage cybersecurity and compliance program effectiveness. The data layer stores and manages data securely, while the integration layer enables seamless data sharing and collaboration. Finally, the infrastructure layer provides the underlying computing resources needed to run the platform and ensure its availability and reliability.

5.4 Hyperproof

Hyperproof is a cybersecurity compliance management platform that helps organizations manage their compliance programs more efficiently. The Hyperproof platform is built on a multi-layered architecture that includes the following layers:

1. **Presentation Layer:** The presentation layer is responsible for presenting the user interface to the user. It includes components such as the web application interface that users interact with to access the Hyperproof platform. This layer is designed to be user-friendly, intuitive, and easy to navigate, enabling users to perform tasks and access the various features of the platform with ease.
2. **Business Logic Layer:** The business logic layer is responsible for implementing the core functionality of the Hyperproof platform. It includes compliance management tools and features that enable organizations to manage their compliance programs effectively. For example, the compliance management tool enables organizations to create, manage, and track compliance tasks and requirements, while the evidence management tool enables organizations to store and manage evidence related to their compliance programs.
3. **Data Access Layer:** The data access layer is responsible for managing the storage and retrieval of data used by the Hyperproof platform. This includes compliance data, such as compliance tasks, requirements, and evidence, as well as user data, such as login credentials and access permissions. This layer ensures that data is securely stored and accessible when needed, with robust data backup and recovery mechanisms in place to prevent data loss.
4. **Integration Layer:** The integration layer provides the mechanisms that enable Hyperproof to integrate with other systems and tools. It includes APIs and other integration components that allow data to be exchanged between Hyperproof and other systems, enabling seamless data sharing and collaboration. For example, Hyperproof can integrate with other compliance tools, such as risk assessment tools and GRC platforms, to provide a more comprehensive view of an organization's compliance program.
5. **Infrastructure Layer:** The infrastructure layer includes the underlying computing resources that support the Hyperproof platform. This includes physical servers, networking equipment, and other infrastructure components needed to host the platform and ensure its availability and reliability. This layer is designed to be scalable and resilient, with multiple redundancies and failover mechanisms in place to ensure that the platform is always available when needed.

In summary, the layers of the Hyperproof architectural model work together to provide a comprehensive compliance management solution that is user-friendly, secure, and scalable. The presentation layer provides the user interface, the business logic layer provides the core functionality, the data access layer manages data storage and retrieval, the integration layer enables system integration, and the infrastructure layer provides the computing resources needed to run the platform.

VI. CONCLUSION

In conclusion, compliance with NIST and FedRAMP standards is critical for companies that provide cloud-based products and services to federal agencies. NIST provides a wide range of guidelines and best practices for cybersecurity, data privacy, AI, physical measurement science, and advanced manufacturing, among other topics. FedRAMP, on the other hand, provides a standardized security assessment process for cloud-based products and services that federal agencies can trust.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 2, March 2023
Impact Factor: 7.301

To be compliant with NIST and FedRAMP, companies must undergo rigorous security assessments, select an accredited third-party assessment organization, prepare and submit a security package, perform a security review, and maintain ongoing compliance. Achieving compliance with NIST and FedRAMP standards can be a significant investment of time and resources, but it can also provide a competitive advantage for companies seeking to sell cloud-based products or services to federal agencies

REFERENCES

[1]. "Cybersecurity framework," NIST, 01-Mar-2023. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: 14-Mar-2023].

[2]. "CyberStrong: CyberSaint Cyber & IT Risk Management software," CyberStrong | CyberSaint Cyber & IT Risk Management Software. [Online]. Available: https://www.cybersaint.io/cyberstrong. [Accessed: 14-Mar-2023].

[3]. "How to become Fedramp authorized," How to Become FedRAMP Authorized | FedRAMP.gov. [Online]. Available: https://www.fedramp.gov/. [Accessed: 14-Mar-2023].

[4]. "HIPAA compliance and Cybersecurity Solutions," HIPAA One, 25-Jan-2023. [Online]. Available: https://hipaaone.com/. [Accessed: 14-Mar-2023].

[5]. "Automated Soc 2, HIPAA, GDPR, Risk Management, & more | drata." [Online]. Available: https://drata.com/. [Accessed: 14-Mar-2023].

[6]. "Automated Security & Compliance Software built for scale," Hyperproof, 02-Mar-2023. [Online]. Available: https://hyperproof.io/. [Accessed: 14-Mar-2023].

[7]. "Cybersecurity & IT Risk and Compliance Software," CyberSaint. [Online]. Available: https://www.cybersaint.io/. [Accessed: 14-Mar-2023].