International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Best Practices for Developing System Security Plans under the NIST Framework

Sabeeruddin Shaik

Independent Researcher
Albany, New York
sksabeer8500@gmail.com

Abstract

To Protect the Information systems in the Organization, to perform Risk Assessments on the systems, and to maintain the security of the systems from rising threats. It is critical and essential to build the Robust System Security Plans. The National Institute of Standards and Technology (NIST) Framework has provided the details structure to build the security plans. Security Plans are most important for Organizations because they provide the components, Details, and Risk appetite of the systems, which help in analysing and improving the security of the systems. Security plans not only serve as compliance tools but also act like a structured framework that aligns with the Organization's objective of improving security. This Research paper analyses the best practices for building security plans that align with compliance regulations, Risk Management, and Organizational Resilience. It also analyses the latest techniques, Tools, and Usage of Artificial Intelligence and automation to improve the effectiveness of Security plans. The key topics that will be discussed in the research paper are Detecting the problems, Mitigation measures, and the Importance of Implementing these measures in building the organization's security posture.

Keywords: System Security Plan, NIST Framework, Cybersecurity, Best Practices, Compliance, Risk Management, Threat Mitigation, Continuous Monitoring

1. Introduction

In this Evolving Modern Digital World, Cyber Threats are increasing. To protect the Organization's Assets, it is important to improve the security standards of the systems that align with the compliance. The System Security Plan provides the complete details of security controls, System owner, and Risk appetite for that specific system. System Security Plans are important for compliance with Frameworks like FISMA, NIST, and some other Frameworks, mainly for industries handling Sensitive or classified Data.But it takes work to build the security plan. Because security plans should align with the compliance regulations, they should satisfy the company policies and Industry standards. With the help of security plans, we perform the Risk Analysis and improve the organization's security posture. So, the plan should be built in such a way that it should be able to collect all the details to perform the Risk Assessment. With the help of the NIST Cybersecurity Framework, this paper analyses all the challenges

in developing System security plans and providessolution. This paper provides a roadmap for Organizations to improve their security posture [1]

A. Problem Statement

Here are a few challenges that might affect building the security system plans

1. **Compliance Regulatory requirements by NIST Cyber security framework-** The Regulatory Frameworks are complex. So, understanding them and aligning the security Plan accordingly might be difficult
2. **To understand the system-** It is important to understand the scope, security controls and components of the specific systems and should be documented accordingly. Not having a proper understanding might lead to security gaps, further making the system vulnerable.[7]
3. **Lack of Risk Assessment Practices -** Risk Assessments must be performed, and a clear picture of Risk appetite should be documented. This way, those Risks can be mitigated, or else they might lead to vulnerability.[2][5]Misalignment of the Security plan with the Cyber security framework and Operational processes. Not following the industry standards.
4. **Lack of Resources-** Many small-scale or medium-scale Industries might not have a Financial Budget, shortage of Employees, or Lack of cyber security professionals; they could not build effective security plans and continuously monitor and update the plans as per the security requirements.
5. **Metrics and Key Performance Indicators (KPI)-**Organizations are lacking in performing the performance metrics of Tools and Security plans, which are leaving gaps in optimizing security.

6. **Lack of Monitoring on Vendor Supply Chain-** Organizations often depend on third-party vendors for critical services and do not maintain due diligence in performing research about vendor security controls, storage security, andsupply chain security. Resulting in risk Transmission from vendors to the Organization.

B. Solutions

By Following a structured approach, the challenges can be resolved. Here are a few solutions:

System classification- The classification of the systems can be done by considering the Confidentiality, Integrity, and Availability factors based on the criticality of the system, which should be classified as Critical, High, Medium, and low. [1].For System classification, Use Federal Information Processing Standards (FIPS-199)[4].Performing Risk Assessment and qualitative and Quantitative Analysis could help determine the Risk factors of the systems and their impacts[2].NIST SP 800-30 Framework can be used to identify the Risks and estimate Risk levels

Structured Implementation- Follow the NIST Framework for the structured approach to select the security controls for the system. Ensure that those security controls also align with the company goals

and Risk tolerance[3].Security controls should act as the preventative measures to mitigate the risks that were outlined through the Risk Assessment

Collaboration with the stakeholders- while preparing security plans, all the departments in the Organization should be considered and satisfy the goals of all the departments. So, it is crucial to work with all departments to collect the required information and build the plan accordingly.[8]

Continuous Monitoring and Improvement- Considering the changing world and Technology, it is important to continuously monitor the security plan and update it accordingly to satisfy current standards and compliance. This could be achievable by following the NIST SP 800-137 Framework.[6].For continuous monitoring, Automated tools can be used to analyse and evaluate the effectiveness of security against emerging threats.

C. Uses

By Implementing the system security plan, the security posture of the Organization can be improved. Regulatory Compliance- Since the Security plan is built following the FISMA, NIST SP 800-171, ISO 27001, ISO 27002 or other Frameworks. The security posture of the Organization will satisfy the Legal and Industry requirements

Effective Risk Management- As the systems are classified based on the criticality. It is easy to prioritize and mitigate the vulnerabilities after performing the Risk Assessment

Stakeholders Awareness - Working with cross-functional teams, asking them questions to collect information, and educating them regarding the security controls and their importance will help employees in different departments become knowledgeable about security measures.

Deploy Robust Security Assessment Tools- Deploying the automated tools to analyse the Risk appetite, to detect the Vulnerabilities and Threats. Tools like FAIR - Factor Analysis of Information Risk, this tool is utilized in the Financial Industries for performing quantitative Risk analysis to analyse and prioritize the Resources. Data analytic models can also be used by creating graphs and charts to compare the potential attack vectors and Based on these automated analysis tools, we can analyse the impacts and implement preventive measures.

Zero Trust Architecture - Implementing the Zero Trust Architecture principles will improve the authentication and authorization capabilities. It makes sure no unauthorized people will have access to the resources because it authenticates every time, even if it is a known device. It works on the principle of zero trust until it gets authenticated. Implementing these principles in the security plan will improve the effectiveness of the plan.

Cross-Functional Teams Collaboration - Create a Team channel and include employees from all departments in developing the security plan. This ensures the concerns of all the departments of the organization are addressed and builds the security plan to overcome the challenges.

Real Time Monitoring- Deploy Automated and AI tools to perform regular monitoring, collect logs and detect anomalies. AI can utilize those patterns and automate responses to those detections, improving the Security plan's effectiveness.

Also Utilize automation to update the security plan if any new security controls are added or changed to

keep the plan updated.

Vendor Risk Management - Develop a security plan for the vendors. So that the third-party vendors could provide the details of the security concerns, and based on that, we could analyse the security functions and determine the supply chain security.

Metrics Driven Evaluation- Perform Key performance Indicator analysis like Mean time to detect, mean time to Respond, and percentage of controls implemented successfully. Through this process, we could analyse the efficiency of tools and frameworks that we are following, update the plan as per metrics, and improve the security controls as per security requirement

Best Practices for Developing system security Plans

System security plans must be built based on the Company scale, Business requirements, Scope, Risk profile, Industry sectorand Expected deliverables.Here are a few points that should be considered in building the Security plan:

Industry specific Control- Security plans must be built as per the industry sector requirements. The plan should satisfy the compliance regulatory requirements of specific Industry. If for example security plan for Health care sectors should emphasize the compliance requirements with HIPAA standards in protecting the data of the patients. In Financial sectors it should satisfy the compliance requirements with GDPR, PCI-DSS and GLBA in protecting the personal information of the customers.[1][4]

Developing Threat Models - Prepare Threat Models based upon the industry sector, System criticality and classification. Consider the MITRE Attack framework in identifying Tactic, Techniques and Procedures relevant to the industry.

Asset Inventory Management - Create an Inventory of the Assets like hardware, software, data, Systems and cloud resources. Perform the data classification and Based on the criticality categorize the Assets and implement asset-specific controls within the Security Plan.[8]

3.Impact

Improved Scalability - A tailored system security plan can be implemented by all scales of Industries from small to Multi-National Corporations and can improve the security of the critical systems in the Organization and protect the data.[3][9]

Improved Incident Response Times - By Deploying the Automated tools for real time monitoring, to detect and mitigate threats. This helps in reducing the response time and improving the recovery capabilities. This will reduce the financial losses and reduce the downtime of the resources.[6]

Alignment with Business Goals - As the security plans are developed with the primary focus in achieving the business goals by improving the security of the organization. This structured approach to the security plan will help in achieving that goal.[8]

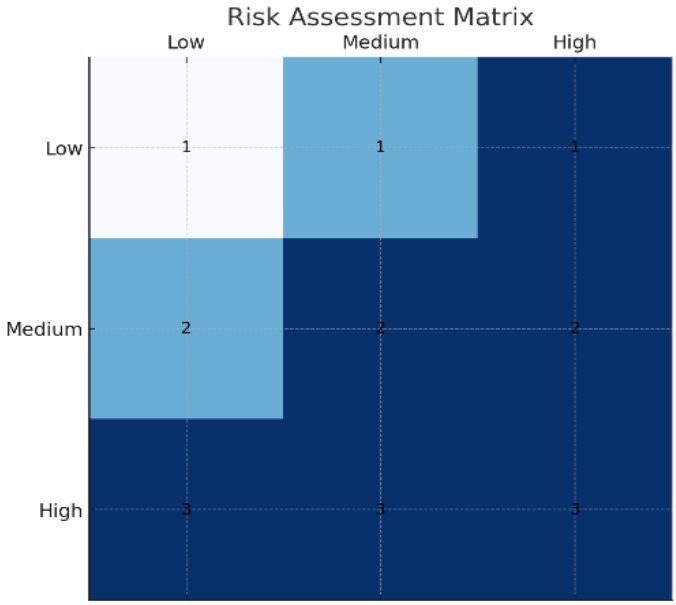
Improved Audit and Reporting Times – By performing the KPI and deploying tools for automating the updating of documentation this improved the adherence to regulatory requirements[6].Building the system security plan and implementing the plan will have many positive impacts on the organizations. The system security plan will help in detecting, Preventing and mitigating the Threats more effectively, which improves the security Postures of the Organization. Continuous monitoring of the systems,

regular security assessments, prioritization of Risks, and mitigation will enhance security.The structured approach and implementation of security will develop trust among stakeholders and improve organizations' reputations.Keeping the security plan up to date and implementingsecurity controls accordingly will prevent emerging threats.

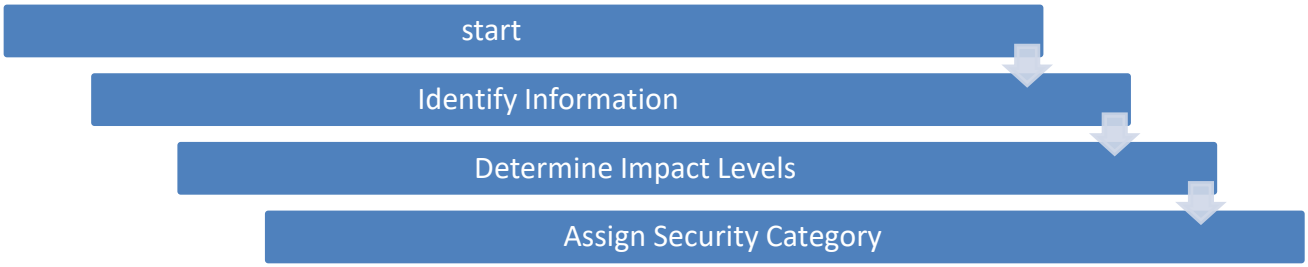
2. Scope

Organizations must build System security plans to mitigate emerging threats and Satisfy compliance requirements. This practice of building security plans is being implemented in various industries, such as Government, Healthcare,Finance, and all other critical sectors. Artificial Intelligence andMachine learning will play a crucial role in automating and developing the system security plans by analysing the Threat Vectors and keeping the security plan updated.System security plans will be integrated with the Cyber Threat Intelligence platforms to analyse the emerging threats and provide real time updates[4][7]

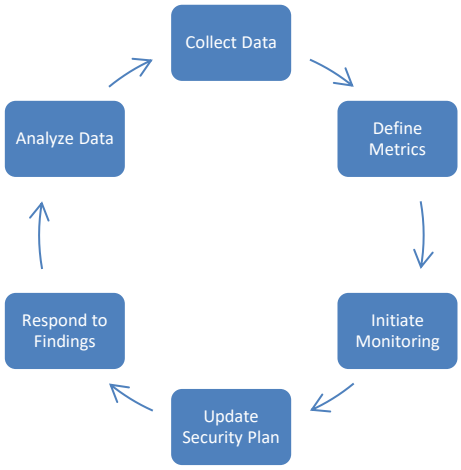
4. Visual aids



(i) Risk Assessment Matrix



(ii) System Categorization Flowchart



(iii) Continuous Monitoring Workflow

5. Conclusion

System security plans, when developed with a tailored approach, will act as a critical foundation in maintaining the security of the organizations. Organizations should build System security plans to improve Defense mechanisms and mitigate emerging Threats. By implementing automated tools, Artificial Intelligence, and Threat Intelligence platforms and utilizing Zero Trust Architecture Principles, Organizations can build resilient and adaptive system security plans. System security plans are developed by following the best practices of the NIST Framework, which addresses mitigating Risks by performing Risk Assessments, working with cross-functional teams, continuous monitoring, and updating the security controls will boost the company's security posture. With these best practices, Organizations can endure long-term security and resilience. Industries should consider this as a continuous program, conduct regular reviews, and develop plans as per the latest cyber threats and compliance regulatory requirements.

6. References

[1] National Institute of standards and Technology, "Guide for Developing security plans for Federal Information systems", NIST (800-18 Revision 1), 2006.

[2] N. I. o. S. a. T. ". a. G. f. i. T. systems", NIST SP 800-30 Revision 1, 2012.

[3] N. I. o. s. a. T. :. a. p. c. f. F. I. s. a. Organizations, NIST SP 800-53 Revision 4, 2013.

[4] F. I. s. M. A. o. 2022, Tittle III of the E-Government Act, 2002.

[5] e. a. R.Ross, Managing Information security Risk :Organization,Mission and Information systems view, NIST SP 800-39, 2011.

[6] N. I. o. s. a. Technology, Information security continuous Monitoring for Federal systems and organizations, NIST SP 800-137, 2011.

[7] A.B.Smith, The Importance of system secuity plans, Journal of cyber security Practices, 2017.

[8] C. J. a. E. Brown, Enhancing Organizational security: A study of NIST implementation, International Journal of Information security, 2018.

[9] R. Green, Integrating Risk Management strategies in System security plans, Journal of Information systems.

[10] N. I. o. s. a. Technology, Framework for improving critical Infrastructure security, NIST CSF, 2014.