Cybersecurity Assessment Report: for systems and organizations

- Useful insights -

April 15, 2023

Contents

1 Scope

The scope of this cybersecurity assessment focuses on identifying vulnerabilities and weaknesses in the organization's cybersecurity posture and providing recommendations for improvement. The assessment is conducted in accordance with the NIST Cybersecurity Framework (CSF) and NIST SP 800-53 controls.

The assessment team conducts a comprehensive evaluation of the organization's information systems, applications, and network infrastructure. The team utilizes a variety of techniques, including penetration testing and vulnerability assessments, to identify potential attack vectors and security weaknesses.

The purpose of the assessment is to provide the organization with an understanding of its current cybersecurity posture and identify areas for improvement. The assessment team provides recommendations to the organization based on the assessment results, aimed at improving the organization's cybersecurity posture and better protecting its systems and data.

The assessment team might identify a number of vulnerabilities and weaknesses in the organization's cybersecurity posture, including outdated software versions, weak passwords, unpatched systems and applications, and weaknesses in physical security measures.

1.1 Workflow

The following workflow outlines the steps involved in conducting a comprehensive cybersecurity assessment:

1. **Methodology -** Select and follow a cybersecurity methodology to guide the assessment process.

2. **Collect Information and Define Scope -** Gather necessary information about the organization's assets, systems, and processes, and define the scope of the assessment. Identify the requirements, assumptions, usage flows, system architecture flows, system components, and system component interactions. Map the information gathered from documentation to the testing environment to determine how to bypass identified requirements and assumptions.

3. **Evaluate Compliance with Security Standards -** Evaluate the organization's compliance with relevant security standards, such as NIST Cybersecurity Framework, NIST SP 800-53, and other industry best practices.

   - **Threats Identification -** Identify potential circumstances or events that could affect the operations and assets of the system through authorized or unauthorized access, resulting in destruction, disclosure, information manipulation, or denial of service. List potential sources of the threat and analyze possible events that could result from these sources. Use past experiences, ethical hacking mindset, and basic methodologies such as NIST 800-53/13, OWASP, and OSSTTM to make educated guesses.

- **Conduct Vulnerability Assessments -** Identify weaknesses and vulnerabilities in the organization's systems and applications using techniques such as penetration testing and vulnerability assessments.
- **Conduct Risk Assessment -** Identify and analyze potential cybersecurity risks to the organization's assets, systems, and processes. See also Section 7.

4. **Results -** The results of the assessment must be presented in two formats: a report containing all technical details and a summary document in the form of an executive summary.
5. **Provide Recommendations -** Provide recommendations for improving the organization's cybersecurity posture, including a prioritized list of actions to take based on the assessment results.

By following this workflow, the cybersecurity assessment team can systematically and comprehensively evaluate the organization's cybersecurity posture and identify areas for improvement. The team can then provide recommendations and prioritize actions to help the organization enhance its security and protect its assets and data.

2 Introduction

This section provides useful background information on the assessment.

The NIST CSF consists of the core framework, implementation tiers, and profiles. Overall, the NIST Cybersecurity Framework is a flexible and adaptable approach to cybersecurity risk management that can be customized to the needs of any organization. By following the framework's guidelines and best practices, organizations can improve their cybersecurity posture and better protect their systems and data.

3 Framework Core

The core framework consists of functions, categories, and subcategories that provide a high-level description of the desired cybersecurity outcomes. The five functions, Identify, Protect, Detect, Respond, and Recover, provide a general approach to cybersecurity that can be applied in any organization. The categories and subcategories provide specific cybersecurity objectives, including physical security, data security, and business results. The Framework is outcome-driven, allowing organizations to implement customized risk-based approaches to achieve the desired outcomes. The text also provides an example of a subcategory and highlights the informative references that organizations can use as guidance to achieve the desired outcomes.

1. **Identify:** The assessment evaluates the organization's ability to understand and manage cybersecurity risks, including asset management, risk assessment, and risk management processes.

2. **Protect:** The assessment evaluates the organization's ability to implement safeguards to protect against cybersecurity threats, including access control, awareness and training, and data security measures.

3. **Detect:** The assessment evaluates the organization's ability to detect cybersecurity threats in a timely manner, including continuous monitoring, anomaly detection, and incident response capabilities.

4. **Respond:** The assessment evaluates the organization's ability to respond to cybersecurity incidents, including incident management, communication, and recovery planning.

5. **Recover:** The assessment evaluates the organization's ability to recover from cybersecurity incidents, including business continuity planning and disaster recovery processes.

4 Framework Tiers

In addition to the core framework, the NIST Cybersecurity Framework includes implementation tiers and profiles. The implementation tiers provide a way for organizations to gauge the maturity of their cybersecurity practices and to identify areas for improvement. The tiers range from Tier 1, which represents partial or inconsistent implementation of cybersecurity practices, to Tier 4, which represents a proactive and adaptive approach to cybersecurity risk management.

1. **Tier 1: Partial -** The organization has limited awareness of cybersecurity risk and has not yet established formal risk management processes.

2. **Tier 2: Risk-Informed -** The organization has a basic understanding of cybersecurity risk and has implemented some risk management practices.

3. **Tier 3: Repeatable -** The organization has established formal risk management processes and regularly assesses and updates its cybersecurity posture.

4. **Tier 4: Adaptive -** The organization has a dynamic and proactive approach to managing cybersecurity risk, including continuous monitoring and refinement of its risk management practices.

5 Framework Profiles

The NIST Cybersecurity Framework Profiles are a critical component of the Framework that allow organizations to customize the Framework to their specific needs, risk management strategies, and resource constraints. Profiles provide a mechanism for organizations to identify the cybersecurity outcomes they wish to achieve and the subcategories from the Framework that are most relevant to their specific circumstances.

In a Profile, organizations can specify their requirements and objectives, including the mission, goals, and priorities of the organization. They can also specify their risk posture and the resources they are willing to allocate to cybersecurity. Once a Profile has been developed, organizations can use it to identify gaps in their cybersecurity posture and to prioritize improvement efforts.

Profiles can be used in a number of ways, including:

1. **Descriptive Profiles -** These Profiles provide a snapshot of an organization's current cybersecurity posture and can be used to identify gaps between the current state and the desired state.

2. **Target Profiles -** These Profiles represent the desired state of an organization's cybersecurity posture and can be used to set goals and priorities for improving cybersecurity.

3. **Implementation Profiles -** These Profiles provide a plan for implementing the Framework within an organization, including prioritized actions and resource requirements.

Profiles can be used in conjunction with the Framework Core and Implementation Tiers to provide a comprehensive approach to cybersecurity risk management. By tailoring the Framework to their specific needs, organizations can better manage cybersecurity risk and improve their overall security posture.

6 Using the NIST CSF Spreadsheet

The NIST CSF provides a spreadsheet tool that can be used to help organizations identify their mission objectives and evaluate their cybersecurity posture. The tool includes a set of functions that can be used to assess an organization's current state, as well as to develop a target state.

To use the spreadsheet, follow these steps:

1. Identify your organization's mission objectives.

2. Cross-check your mission objectives with the functions listed in the NIST CSF spreadsheet.

3. For each function, assign a value of "High," "Moderate," or "Low" based on how well the function is currently being performed in your organization.

4. Calculate an overall score for each category (Identify, Protect, Detect, Respond, and Recover) based on the assigned values.

5. Use the scores to develop a roadmap for improving your organization's cybersecurity posture.

When assigning values to each function, it is important to be honest and objective. Remember that the goal is not to achieve perfect scores, but to identify areas that need improvement and to develop a plan for addressing them.

The Framework aims to align Functions, Categories and Subcategories with the organisation's business requirements, risk tolerance and resources. An example of the application of the spreadsheet in the transport sector can be found at this link "How to Use the Cybersecurity Framework Profile for Connected Vehicle Environments".

7 Risk Evaluation

Risk evaluation is a critical component of the cybersecurity assessment process. It involves assessing the likelihood and impact of potential threats to the organization's assets and systems.

The NIST Cybersecurity Framework (CSF) does not prescribe a specific risk assessment methodology, but it does provide a framework for organizations to manage and reduce their cybersecurity risks. To evaluate risks within the context of the CSF, NIST SP 800-30 provides guidance on conducting risk assessments. Using NIST SP 800-30, organizations can identify, assess, and prioritize risks that are relevant to their goals and objectives. Then, they can apply the CSF's functions, categories, and subcategories to address those risks. It's important to note that the CSF and NIST SP 800-30 should be used in conjunction with each other to support an organization's risk management process.

7.1 Likelihood Levels

The likelihood of a cybersecurity incident refers to the probability that the threat will occur. To evaluate likelihood, the assessment team should consider factors such as historical data, threat intelligence, and vulnerability assessment. The likelihood levels used in this assessment are based on NIST SP 800-30.

1. **Low likelihood:** The threat is unlikely to occur, or it is highly improbable.

2. **Moderate likelihood:** The threat is possible, but it is not expected to occur frequently.

3. **High likelihood:** The threat is likely to occur, or it is highly probable.

7.2 Impact Levels

The impact of a cybersecurity incident can vary widely, depending on the type of incident and the assets or systems affected. Therefore, it is essential to assign a severity level to each potential impact so that the organization can prioritize its response efforts. To evaluate impact, the assessment team should consider the potential consequences of a cybersecurity incident, including operational, financial, reputational, and legal impacts. The impact levels used in this assessment are based on NIST SP 800-30.

1. **Low impact:** The cybersecurity incident has a minimal effect on the organization's operations, financials, reputation, or legal compliance.

2. **Moderate impact:** The cybersecurity incident has a noticeable effect on the organization's operations, financials, reputation, or legal compliance.

3. **High impact:** The cybersecurity incident has a significant effect on the organization's operations, financials, reputation, or legal compliance.

7.3 Risk Matrix

A risk matrix is a tool that combines the likelihood and impact levels of a cybersecurity incident to assign a risk level. In this assessment, a risk matrix based on the NIST SP 800-30 is used to assign a risk level to each identified cybersecurity risk. The risk matrix consists of a table with the likelihood levels along one axis and the impact levels along the other axis. The intersection of these levels produces a risk level, which is typically categorized as low, moderate, or high.

Risk Level	**Likelihood**	**Impact**	**Description**
High	High	High	A cybersecurity incident is likely to have significant impact on the organization.
	High	Moderate	A cybersecurity incident is likely to have noticeable impact on the organization.
	Moderate	High	A cybersecurity incident is possible and likely to have significant impact on the organization.
	Moderate	Moderate	A cybersecurity incident is possible and likely to have noticeable impact on the organization.
Moderate	Low	High	A cybersecurity incident is unlikely but may have significant impact on the organization.
	High	Low	A cybersecurity incident is likely but may have minimal impact on the organization.
	Moderate	Moderate	A cybersecurity incident is possible but may have minimal impact on the organization.
	Low	Low	A cybersecurity incident is unlikely and may have minimal impact on the organization.
Low	Low	Moderate	A cybersecurity incident is unlikely but may have noticeable impact on the organization.
	Moderate	Low	A cybersecurity incident is possible but may have minimal impact on the organization.
	Low	Low	A cybersecurity incident is unlikely and may have minimal impact on the organization.

Table 1: Risk matrix based on NIST SP 800-30.

The risk matrix can be used to prioritize the cybersecurity risks identified during the assessment, with higher risk levels indicating a need for more urgent and immediate action. The assessment team can use the risk matrix to communicate the risk level to stakeholders and decision-makers in a clear and concise way, helping them to understand the potential impact of cybersecurity incidents and make informed decisions about risk management.

8 Results

This section provides an overall summary of the assessment results, including key findings and security mitigation.

9 Recommendations

This section provides detailed recommendations for improvement, including specific actions that the organization can take to improve its cybersecurity posture.

References

The following NIST publications were used in the assessment process:

[1] NIST Cybersecurity Framework: `https://www.nist.gov/cyberframework`

[2] NIST SP 800-30, Guide for Conducting Risk Assessments: `https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf`

[3] NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf`

A Appendix

A.1 NIST SP 800-53 Controls

This section provides an assessment of the organization's cybersecurity posture against the NIST SP 800-53 controls. The assessment team should review each control and evaluate the organization's compliance with each control.

1. **Access Control:** The assessment evaluates the organization's access control measures, including password policies, user authentication, and access control technologies such as firewalls and intrusion prevention systems.

2. **Awareness and Training:** The assessment evaluates the organization's employee cybersecurity awareness training program and its effectiveness in improving cybersecurity awareness and behavior.

3. **Audit and Accountability:** The assessment evaluates the organization's audit and accountability measures, including logging, auditing, and monitoring of system activity.

4. **Configuration Management:** The assessment evaluates the organization's configuration management processes, including configuration control, configuration identification, and configuration status accounting.

5. **Identification and Authentication:** The assessment evaluates the organization's identification and authentication measures, including the use of multifactor authentication, password policies, and biometric identification technologies.

6. **Incident Response:** The assessment evaluates the organization's incident response plan, including the incident response team, procedures for reporting incidents, and incident response technologies.

7. **Maintenance:** The assessment evaluates the organization's maintenance processes, including patch management, system updates, and system backups.

8. **Media Protection:** The assessment evaluates the organization's media protection measures, including physical security of media, encryption of data in transit and at rest, and secure disposal of media.

9. **Personnel Security:** The assessment evaluates the organization's personnel security measures, including background checks, security clearances, and termination procedures.

10. **Physical and Environmental Protection:** The assessment evaluates the organization's physical and environmental protection measures, including access control to physical facilities, environmental controls for systems, and protection against natural disasters.

11. **Risk Assessment:** The assessment evaluates the organization's risk assessment processes, including identification of risks, analysis of risks, and evaluation of risks.

12. **Security Assessment and Authorization:** The assessment evaluates the organization's security assessment and authorization processes, including security testing, vulnerability scanning, and authorization to operate processes.

13. **System and Communications Protection:** The assessment evaluates the organization's system and communications protection measures, including encryption of data in transit, network segmentation, and protection against malware and other cyber threats.

14. **System and Information Integrity:** The assessment evaluates the organization's system and information integrity measures, including integrity checking of systems and data, protection against malware and other cyber threats, and intrusion detection and prevention technologies.

By incorporating NIST SP 800-53 controls into the assessment report, the organization can gain a more comprehensive understanding of its cybersecurity posture and identify areas where improvements can be made to align with industry best practices.