NIST Cyber Security Review

The NIST Cybersecurity Review (NCSR) is a structured assessment framework designed to help organizations evaluate, manage, and improve their cybersecurity maturity. It is based on the NIST Cybersecurity Framework (CSF), which provides guidelines to protect organizations from cyber threats. The NCSR is widely used by government agencies, financial institutions, healthcare providers, and enterprises to assess their cybersecurity capabilities and ensure compliance with industry standards.

Why is NIST Cybersecurity Review Important?

- Identifies gaps in cybersecurity posture.
- Aligns cybersecurity practices with industry standards.
- Helps in risk management and compliance.
- Strengthens incident response and threat detection.
- Supports continuous security improvements.

Example: A banking institution conducting an NCSR assessment might discover weaknesses in its access control policies and implement multi-factor authentication (MFA) to enhance security.

NIST Cybersecurity Review Process

The NCSR process follows a structured approach to assess, implement, and improve cybersecurity measures. It consists of five key phases:

1. Identify – Understanding Risks & Assets

In this phase, organizations must identify critical assets, risks, and business operations to establish a cybersecurity foundation.

Key Activities:

- Asset inventory (databases, servers, cloud resources).
- Identify cybersecurity risks and compliance requirements.
- Define roles & responsibilities within the security team.
- Develop a risk management strategy.

Example: A healthcare organization conducting an NCSR identifies patient data as a critical asset and ensures it is stored securely following HIPAA regulations.

Tools Used:

- CMDB (Configuration Management Database) – ServiceNow, SolarWinds.
- Risk Management Platforms – RSA Archer, LogicGate.

2. Protect – Implementing Security Controls

Organizations must implement protective measures to ensure data integrity, system security, and employee awareness.

Key Activities:

- Access control policies (role-based access control).
- Data encryption and secure cloud storage.
- Network segmentation and firewall implementation.
- Security awareness training for employees.

Example: A retail company encrypts customer credit card data using TLS/SSL to prevent cyber fraud.

Tools Used:

- Identity & Access Management (IAM) – Okta, Microsoft Entra ID.
- Data Loss Prevention (DLP) – Symantec, Forcepoint.
- Endpoint Security – Microsoft Defender, CrowdStrike.

3. Detect – Identifying Cyber Threats

This phase involves continuous monitoring of security events and abnormal activities to detect cyber threats.

Key Activities:

- Real-time monitoring of security logs and network traffic.
- Implementing Security Information and Event Management (SIEM).
- Threat intelligence and anomaly detection.

Example: A financial services company detects a possible DDoS attack using a SIEM tool and mitigates it by diverting traffic through a Web Application Firewall (WAF).

Tools Used:

- SIEM – Microsoft Sentinel, Splunk, QRadar.
- Intrusion Detection Systems (IDS) – Snort, Suricata.
- Threat Intelligence – Recorded Future, Anomali.

4. Respond – Handling Security Incidents

Organizations must establish an incident response plan to mitigate cyberattacks efficiently.

Key Activities:

- Develop a structured Incident Response Plan (IRP).

- Conduct forensic investigations after an attack.
- Report security breaches to stakeholders.

Example: A government agency dealing with a ransomware attack follows an incident response plan to isolate affected machines, restore backups, and report the breach.

Tools Used:

- Incident Response – IBM Resilient, Palo Alto Cortex XSOAR.
- Forensics – Autopsy, EnCase.

5. Recover – Restoring Operations After an Attack

This phase ensures business continuity by restoring compromised systems and improving security measures.

Key Activities:

- Data backup and disaster recovery strategies.
- Conducting a post-incident analysis.
- Updating cybersecurity policies.

Example: A cloud service provider restores business operations from secure backups after a cyberattack, ensuring minimal downtime.

Tools Used:

- Backup & Recovery – Veeam, Acronis.
- Business Continuity Planning – Archer, Fusion Risk Management.

Benefits of NIST Cybersecurity Review

- Provides a structured framework for cybersecurity.
- Enhances compliance with regulations (GDPR, HIPAA, PCI DSS).
- Improves threat detection and response capabilities.
- Ensures continuous monitoring and proactive security.

Implementing an NCSR (National Cyber Security Review) Assessment for Your Organization

The National Cyber Security Review (NCSR) is a framework designed to evaluate an organization's cybersecurity maturity based on NIST Cybersecurity Framework (CSF) principles. It helps organizations identify, assess, and mitigate cybersecurity risks effectively.

Steps to Implement an NCSR Assessment

1. Define the Scope and Objectives

- Determine the business units, departments, or systems to be assessed.
- Align the assessment with regulatory compliance needs (e.g., GDPR, ISO 27001).
- Identify key stakeholders (CISO, IT Security Team, Compliance Officers).

2. Gather Required Documentation

Prepare essential security documents, including:

- Risk Management Policies
- Incident Response Plans
- Access Control Policies
- Security Awareness Training Records
- Third-Party Security Agreements

3. Conduct Self-Assessment Using NIST CSF

The NCSR assessment aligns with five key NIST CSF functions:

1. **Identify** – Understanding risks & assets (e.g., asset inventory, risk assessments).
2. **Protect** – Implementing safeguards (e.g., encryption, firewalls, MFA).
3. **Detect** – Monitoring threats (e.g., SIEM, IDS, log management).
4. **Respond** – Managing incidents (e.g., incident response plans, forensics).
5. **Recover** – Ensuring business continuity (e.g., disaster recovery, backups).

Use the NCSR questionnaire to rate your organization's maturity across these domains.

4. Evaluate Current Cybersecurity Maturity Level

NCSR uses a **maturity model** to assess cybersecurity posture:

- **Partial (1)** – Ad-hoc cybersecurity approach.
- **Risk Informed (2)** – Basic security measures in place.
- **Repeatable (3)** – Documented policies and controls.
- **Adaptive (4)** – Continuous security improvements.

5. Identify Gaps and Areas for Improvement

- Compare your current maturity level with the desired target state.
- Identify cybersecurity weaknesses (e.g., outdated security controls, lack of employee training).
- Prioritize security improvements based on risk impact and feasibility.

6. Develop an Action Plan

- Create a cybersecurity improvement roadmap, including:
- Policy Enhancements – Strengthening security policies and frameworks.
- Technical Controls – Implementing SIEM, XDR, EDR for better threat detection.
- Security Awareness Training – Educating employees on cyber threats.
- Incident Response Drills – Conducting tabletop exercises for preparedness.

7. Conduct Continuous Monitoring & Reporting

- Implement a Security Operations Center (SOC) or monitoring tools.
- Use SIEM solutions like Microsoft Sentinel, Splunk, or QRadar to detect threats.
- Perform regular NCSR reassessments (annually or biannually) to measure improvements.
- Report findings to executives and regulatory bodies for compliance tracking.

Conclusion

Implementing an NCSR Assessment helps organizations enhance their cybersecurity maturity, comply with regulations, and reduce cyber risks. By following a structured approach using NIST CSF principles, organizations can ensure a strong security posture.

Cybersecurity Roadmap Based on NCSR Assessment

A well-structured cybersecurity roadmap ensures that your organization progresses towards a mature and resilient security posture. Based on your NCSR (National Cyber Security Review) assessment results, here's a step-by-step action plan to enhance your cybersecurity maturity.

Phase 1: Immediate Actions (0-3 Months)

Objective: Address critical security gaps identified in the NCSR assessment.

1. Strengthen Security Policies & Compliance

- Update Cybersecurity Policies – Align with NIST CSF, ISO 27001, GDPR standards.
- Risk Assessment Framework – Implement a structured risk management program.
- Regulatory Compliance Review – Ensure compliance with industry-specific regulations.

Tools: NIST RMF, FAIR Model, Cyber Risk Management Platforms (Archer, MetricStream)

2. Implement Basic Security Controls

- Multi-Factor Authentication (MFA) – Enable MFA for all users.
- Endpoint Security – Deploy EDR solutions (CrowdStrike, Microsoft Defender, SentinelOne).
- Patch Management – Automate patching for OS, applications, and firmware.
- Secure Email Gateway – Implement phishing protection (Proofpoint, Mimecast).

Tools: Qualys, Tenable Nessus, Microsoft Intune, Splunk

Phase 2: Intermediate Measures (3-6 Months)

Objective: Improve monitoring, detection, and incident response.

3. Deploy Advanced Threat Detection & SIEM

- Implement SIEM (Security Information and Event Management)
    - Centralize log management & real-time threat detection.
    - Recommended SIEM: Microsoft Sentinel, Splunk, QRadar.
- SOC (Security Operations Center) Setup
    - Deploy 24/7 monitoring or outsource to a Managed Security Services Provider (MSSP).

Tools: MITRE ATT&CK, IBM X-Force, Threat Intelligence Feeds (VirusTotal, AlienVault)

4. Conduct Security Awareness & Training

- Phishing Simulation Campaigns – Train employees to recognize threats.
- Security Awareness Training – Use platforms like KnowBe4, Infosec IQ.

Tools: KnowBe4, Infosec IQ, Cyber Range Exercises

Phase 3: Long-Term Cybersecurity Maturity (6-12 Months)

Objective: Build a sustainable and proactive security strategy.

5. Implement Zero Trust & Cloud Security

- Zero Trust Architecture – Enforce least privilege access control.
- Cloud Security Posture Management (CSPM) – Secure Azure, AWS, GCP.

Tools: Microsoft Defender for Cloud, Prisma Cloud, AWS Security Hub

6. Enhance Incident Response & Forensics Capabilities

- Automated Incident Response Playbooks – Integrate SOAR (Security Orchestration, Automation, and Response).
- Tabletop Exercises & Red Teaming – Simulate real-world attacks.

🛠 **Tools**: Splunk Phantom, Palo Alto XSOAR, IBM Resilient

Phase 4: Continuous Improvement & Compliance (Ongoing)

Objective: Continuously improve, reassess risks, and stay compliant.

7. Regular Cybersecurity Assessments & Audits

- Conduct Annual Penetration Testing & Vulnerability Assessments.
- Perform Regular NCSR Self-Assessments to track progress.
- Audit Third-Party Vendors for Security Risks.

🛠 **Tools**: Qualys, Rapid7, Nessus, CISA Cyber Hygiene