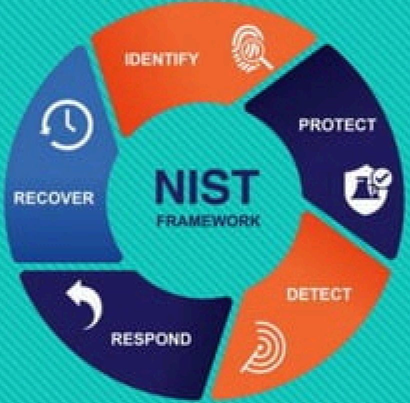
Conducting a NIST Cybersecurity Framework (CSF) Assessment



Nicholas Davis
CISSP, CISA, CRISC, CCSP, HCISPP
March 6, 2024

Nicholas Davis
CISSP, CISA, CRISC, CCSP, HCISPP

- 25 years of cybersecurity experience developing and implementing comprehensive information security programs
- Providing strategic guidance and consultation: Advising leadership on security issues, threats, and mitigation strategies.
- Assessment and audit background in NIST, ISO, PCI, HIPAA, GDPR

Strengthen Your Cybersecurity Posture with NIST CSF Assessment

- Identify and manage cybersecurity risks: The framework helps you systematically identify vulnerabilities and prioritize your efforts to address them.
- Improved compliance: By aligning your security practices with the framework, you can demonstrate compliance with relevant regulations and industry standards.
- Enhanced communication: The framework provides a common language for discussing cybersecurity across different departments and stakeholders.

NIST CSF Assessment Process Overview

- Five Core Functions: The framework is organized around five core functions: Identify, Protect, Detect, Respond, and Recover.
- Categories and Subcategories: Each function is further divided into categories and subcategories, providing a detailed framework for assessing your security posture.

Benefits of Conducting a NIST CSF Assessment

- Enhanced decision-making: Gain insights to make informed decisions about your cybersecurity investments.
- Improved resilience: Strengthen your ability to respond to and recover from cyberattacks.
- Increased stakeholder confidence: Demonstrate your commitment to cybersecurity best practices.

Let's Get Started!

- I am an experienced cybersecurity professional with extensive knowledge of the NIST CSF framework.
- I can guide you through the assessment process and help you achieve your security goals.

What is the NIST CSF?

- The NIST CSF is a voluntary framework developed by the National Institute of Standards and Technology.
- It provides a flexible, risk-based approach to help organizations manage their cybersecurity risks.
- The framework consists of five core functions:
- Identify: Identify critical assets and their dependencies.
- Protect: Implement safeguards to protect those assets.
- Detect: Detect security events.
- Respond: Respond to security incidents.
- Recover: Recover critical capabilities after an incident.

Preparing for the Assessment

- Define the scope: Specify the systems, assets, data, and functions to be assessed.
- Gather information: Collect relevant documentation, policies, procedures, and risk assessments.
- Assemble the assessment team: Include individuals with expertise in security, business processes, and risk management.

Identify Function

- Identify critical assets and their dependencies.
- Document risk management processes.
- Analyze business environment and supply chain.

Protect Function

- Review security controls for access control, data security, and information protection.
- Evaluate awareness and training programs.
- Assess protective technology implementation.

Detect Function

- Evaluate security continuous monitoring and detection processes.
- Test anomaly and event detection capabilities.

Respond Function

- Review incident response plan and procedures.
- Assess communication protocols and recovery procedures.

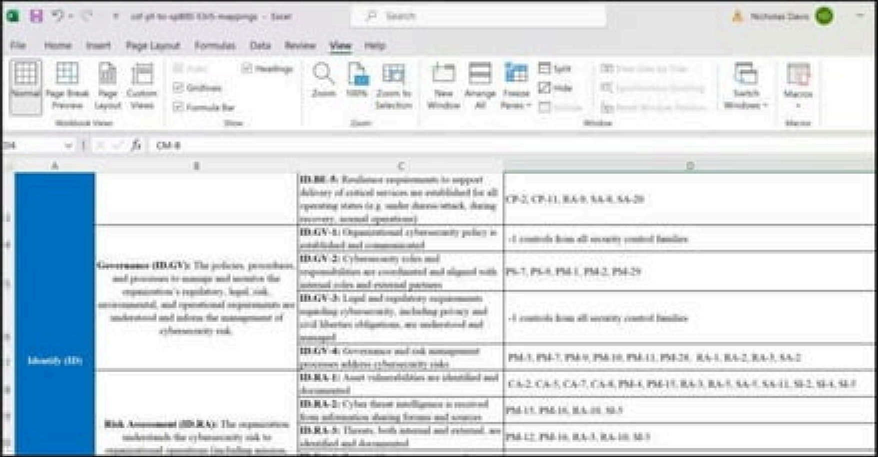
Recover Function

- Evaluate data recovery and restoration plans.
- Assess business continuity and disaster recovery capabilities.

Documenting and Reporting

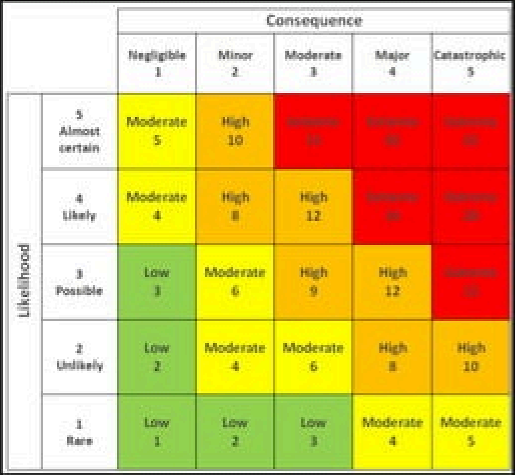
- Document the findings of the assessment for each function.
- Identify areas of strength and areas for improvement.
- Develop a remediation plan to address identified gaps.
- Report the assessment findings to relevant stakeholders.

Controls Assessment



A	B	C	D
Identify (ID)		**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	CP-2, CP-11, RA-9, SA-8, SA-20
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	-1 controls from all security control families
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	PS-7, PS-9, PM-1, PM-2, PM-29
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	-1 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission,	**ID.RA-1:** Asset vulnerabilities are identified and documented	CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	PM-15, PM-16, RA-10, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	PM-12, PM-16, RA-3, RA-10, SI-5

Risk Ranking



		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	[illegible]	[illegible]	[illegible]
	4 Likely	Moderate 4	High 8	High 12	[illegible]	[illegible]
	3 Possible	Low 3	Moderate 6	High 9	High 12	[illegible]
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Reporting to Senior Leadership

- A NIST CSF report to senior leadership should be concise, informative, and actionable. It should highlight the key findings of the assessment and provide recommendations for improvement, all in a language understandable to a non-technical audience.

Discussion

- Questions
- Comments
- Next Steps

End of Presentation