SOURCEPASS™

Contact Us

CYBER ADVISORY SERVICES

NIST Cybersecurity Framework (CSF) Risk Assessment

Strengthen Your Organization's Cybersecurity Posture with a Comprehensive Risk Assessment

What is a NIST Cybersecurity Framework (CSF) Risk Assessment?

The NIST Cybersecurity Framework (CSF) is a recognized industry standard that provides a structured, best-practice approach to managing cybersecurity risk. Version 2.0 introduces the Govern function, making it a more holistic tool for organizations to strengthen their cybersecurity defenses.

The NIST CSF Risk Assessment from Sourcepass evaluates your organization's cybersecurity posture across the Identify, Protect, Detect, Respond, Recover, and Govern functions, providing actionable insights to protect sensitive information and minimize cybersecurity risks.

Key Benefits of the NIST CSF Risk Assessment

Tailored Risk Strategy:

Develop a customized cybersecurity strategy based on your organization's unique risks, mission, and operational needs.

Clear Risk Management Policies:

Establish defined, repeatable policies that align with your organization's current cybersecurity threat environment and regulatory obligations.

Actionable Cybersecurity Insights:

Receive prioritized recommendations and risk findings that help guide your cybersecurity strategy and improve operational readiness.

Holistic Risk Management:

Understand the risks posed by internal and external factors—including supply chain vulnerabilities—and implement effective strategies for managing these risks.

The NIST CSF 2.0 Framework: A Structured Approach to Cybersecurity

The NIST CSF 2.0 comprises six core functions to manage cybersecurity risk:

Identify: Understand your organization's cybersecurity risks and establish a clear baseline for defense.
Protect: Implement measures to protect critical systems and data from cyber threats.
Detect: Build the capability to monitor, detect, and respond to security incidents in real-time.
Respond: Establish incident response protocols to mitigate the impact of a cyberattack.
Recover: Develop plans to restore operations after an incident to reduce downtime and damage.
Govern: Manage risk governance to ensure continuous oversight, adaptability, and alignment with business objectives.

SOURCEPASS™

Contact Us

CYBER ADVISORY SERVICES

NIST Cybersecurity Framework (CSF) Risk Assessment

Strengthen Your Organization's Cybersecurity Posture with a Comprehensive Risk Assessment

NIST Cybersecurity Framework

FUNCTION	CATEGORY	CATEGORY ID
GOVERN (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
IDENTIFY (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
PROTECT (PR)	Identity Management, Authentication, Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
DETECT (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
RESPOND (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
RECOVER (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

SOURCEPASS™

Contact Us

CYBER ADVISORY SERVICES

NIST Cybersecurity Framework (CSF) Risk Assessment

Strengthen Your Organization's Cybersecurity Posture with a Comprehensive Risk Assessment

Scope of Engagement

Sourcepass conducts a thorough risk assessment over several 60–90 minute sessions. During these sessions, we evaluate the IT security controls, policies, and procedures in place at your organization, analyzing your cybersecurity landscape with a focus on the following:

- **Information Technology Department** and its role in the overall cybersecurity program.
- **Existing cybersecurity policies**, plans, and response procedures.
- **Relevant documentation**, including risk management and security incident plans.

Assessment Deliverables

- **Prioritized Risk Findings:** A detailed breakdown of identified risks and gaps in your cybersecurity posture, along with actionable recommendations and priorities for improvement.
- **Customized Risk Strategy:** A tailored cybersecurity strategy based on your organization's unique risks, mission objectives, and threat environment.
- **Cybersecurity Supply Chain Risk Management: A** strategy for overseeing suppliers, customers, and partners, ensuring continuous oversight and analysis of risks in your extended ecosystem.

Outcomes and Recommendations

Our evaluation of your cybersecurity posture against the NIST CSF 2.0 identifies key opportunities for improvement.

We provide:

- **Actionable Recommendations:** Specific, high-priority actions tailored to your organization's cybersecurity needs.
- **Risk Prioritization:** Clear prioritization of cybersecurity risks based on severity, materiality, and impact on your organization.
- **Continuous Improvement:** Guidance for establishing a culture of continuous improvement, with regular updates and reviews of policies and procedures to align with evolving threats and regulations.

SOURCEPASS™

Contact Us

CYBER ADVISORY SERVICES

NIST Cybersecurity Framework (CSF) Risk Assessment

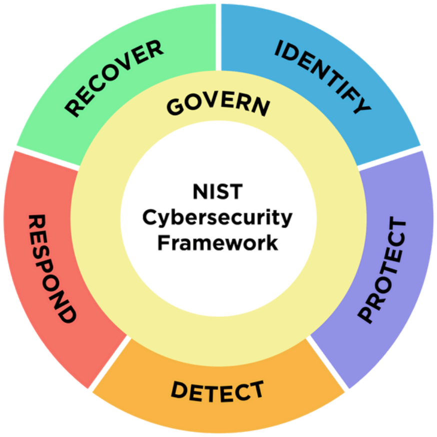
Strengthen Your Organization's Cybersecurity Posture with a Comprehensive Risk Assessment

Why Sourcepass?

Sourcepass Professional Services offers a comprehensive evaluation using the NIST CSF 2.0, leveraging a series of tailored assessments and in-depth evaluations that address your specific cybersecurity needs. Our approach ensures that your organization is not only prepared for current cybersecurity challenges but is also resilient in the face of emerging threats.

Sourcepass's **NIST CSF Risk Assessment** is designed to offer a comprehensive, tailored evaluation of your organization's cybersecurity strengths and areas for improvement.

We don't just identify problems—we provide solutions, offering practical, prioritized steps to strengthen your defenses, minimize risk, and improve overall cybersecurity maturity.



Ready to Strengthen Your Cybersecurity Strategy?

Contact Sourcepass today to schedule your NIST Cybersecurity Framework Risk Assessment and take the first step in safeguarding your organization against evolving cyber threats.

Let us help you prioritize your cybersecurity efforts and build a more resilient, secure environment for your business.