



NIST CSF SERVICE BRIEF

Prioritize Risk. Direct Strategy. Drive Value.

SPECIALIZED **S|3** SECURITY SERVICES

COMPLIANCE ASSESSMENT SERVICES

Your compliance journey shouldn't feel like a maze.

At S3 Security, we translate complex frameworks like NIST, PCI, ISO, and CMMC into clear, actionable steps that align with your business priorities.

Whether you're navigating new regulations or validating existing controls, our experienced team provides the clarity and confidence you need to move forward.

EXPERTISE YOU CAN TRUST

Our team of seasoned Assessors brings deep experience in third-party cybersecurity and compliance. With extensive experience across regulated sectors including healthcare, finance, retail, and other highly regulated industries, they understand how to navigate complexity and deliver results that withstand scrutiny.

THOUSANDS OF SUCCESSFUL ASSESSMENTS

As a compliance leader, we've guided organizations across industries through thousands of regulatory assessments and validations.

TAILORED TO YOUR BUSINESS

No two organizations are alike. We take time to understand your risk profile, operational needs, and data protection priorities—delivering recommendations that are both strategic and practical.

We don't just help you meet compliance standards—we help you use them to strengthen your business.



NIST CYBERSECURITY FRAMEWORK (CSF) 2.0 ASSESSMENT

The NIST Cybersecurity Framework (CSF) 2.0 provides comprehensive guidance for organizations to effectively manage cybersecurity risks.

A NIST CSF Assessment evaluates your cybersecurity posture across six key functions: Govern, Identify, Protect, Detect, Respond, and Recover.

This structured framework helps organizations identify strengths, address weaknesses, and close gaps in their security practices.



Beyond improving cybersecurity readiness, the assessment enables organizations to demonstrate accountability to stakeholders, enhance regulatory compliance, and proactively mitigate risks.

It serves as a roadmap for continuous improvement and alignment with globally recognized cybersecurity standards.

NIST CSF 2.0 ASSESSMENT MATURITY

The NIST CSF 2.0 assessment includes a determination of security maturity which focuses on part or all the strategic and technical aspects of an information security program.

The Assessment identifies the level of maturity of the information security program and the organization's ability to comply with existing requirements.

S3 Security will assess the maturity level for each of the review criteria.

A higher maturity level can only be attained if the previous maturity level is achieved.



NIST CSF 2.0 ASSESSMENT METHODOLOGY

The NIST Cybersecurity Framework (CSF) 2.0 Assessment is broken down into four project milestones:



1 Define Assessment Scope Based on Existing Requirements

2 Evaluate Current State of Client
(Interviews & Testing)

3 Evidence Gathering & Review

4 Results Generation
(Gauge against NIST CSF Target State, Report Completion, Recommendations, Project Plan & Remediation guidance)

NIST CSF REPORT SAMPLE

EXECUTIVE SUMMARY

[Client] engaged Specialized Security Services, Inc. (hereinafter, S3) to perform an information security risk and maturity assessment based on the NIST Cybersecurity Framework (CSF) 2.0. S3 assessed [Client]’s current information security program with respect to confidentiality, integrity and availability of protected information in the enterprise against NIST CSF 2.0 and has provided a gap analysis and maturity rating.

S3 interviewed key data owners and stakeholders to assess [Client]’s maturity and to develop a set of recommendations for improving IT security controls. This report summarizes the assessment of the environment as of [Date]. The objective was to support enterprise goals for data protection, compliance and IT governance and to limit and mitigate any current risks to provide a more secure environment while raising awareness of potential security risks, threats and vulnerabilities to company assets.

[Client] demonstrated a mature level of adherence to the CSF and satisfies the control objectives in all key areas. [Client] was also able to demonstrate well-developed and mature processes around compliance management and reporting which provide validation that operating procedures and security controls are operating within acceptable limits. The risk culture present shows a solid security base and demonstrates mature processes around Awareness & Training, and Data Security.

As a result, S3 has concluded that [Client] ’s overall Cybersecurity Maturity is currently at Level 4 – Measured, per the table below. Opportunities for improvement exist in the area of Supply Chain Risk Management, Incident Response, and Asset Management.



CONFIDENTIAL; NOT FOR DISTRIBUTION

2

OVERALL MATURITY SCORING – FUNCTION AND CATEGORY

The NIST CSF 2.0 is an industry standard control framework that is used by organizations to manage and assess a cybersecurity program. The NIST CSF 2.0 is used by organizations to assess and improve their ability to govern, identify, protect, detect, respond, and recover from cyber attacks. The CSF consists of six (6) core functional areas, 22 categories and 106 subcategories. The graphic below highlights the 6 core functions and 22 categories that makeup these functions:

NIST CSF									
Govern (GV)		Identify (ID)		Protect (PR)		Detect (DE)		Respond (RS)	
Organizational Context (GV.OC)	4.4	Asset Management (ID.AM)	4.2	Identify Management, Authentication, & Access Control (PR.AA)	4.9	Adverse Event Analysis (DE.AE)	4.6	Incident Management (RS.MA)	4.4
Risk Management Strategy (GV.RM)	4.2	Risk Assessment (ID.RA)	4.8	Awareness & Training (PR.AT)	5.0	Continuous Monitoring (DE.CM)	4.9	Incident Analysis (RS.AN)	4.6
Roles, Responsibilities, & Authorities (GV.RR)	4.1	Improvement (ID.IM)	4.7	Data Security (PR.DS)	5.0			Incident Response Reporting & Communication (RS.CO)	3.8
Policy (GV.PO)	5.0			Platform Security (PR.PS)	5.0			Mitigation (RS.MI)	3.8
Oversight (GV.OV)	4.8			Technology Infrastructure Resilience (PR.IR)	5.0				
Cybersecurity Supply Chain Risk Management (GV.SC)	4.0								
								Incident Recovery Plan Execution (RC.RP)	4.8
								Incident Recovery Communication (RC.CO)	4.5

CONFIDENTIAL; NOT FOR DISTRIBUTION

12

NIST CSF REPORT SAMPLE

MOBILE DEVICE MANAGEMENT (MDM)

Description	
Specialized Security Services, Inc. identified that mobile device requirements and configurations are implemented inconsistently. The enforcement of MDM on all devices is incomplete. While some procedures are in place, limitations on personal devices and should be more robust. Explore Mobile Application Management on personal devices as an alternative.	
Key Activities & Prerequisites	
Sub Initiatives	Prerequisites
Review policies and procedures: Review policies and procedures regarding mobile device management.	Policies and Procedures
Update policies and procedures: Update policies to include detailed requirements for mobile devices that will hold [Client] data. Document configurations.	Updated Policies and Procedures
Communicate: Communicate MDM or MAM requirements on all devices.	

	Q4 2024	Q1 2025	Q2 2025	Q3 2025	Q4 2025
TIMELINE					

CONFIDENTIAL; NOT FOR DISTRIBUTION

21

Key Stakeholder Group	
Business Units / IT Security	
Prioritization	
Maturity Impact	High
Risk Reduction	High
Est. Level of Effort	Medium
Sample Operational Metrics	
% of systems with MDM solution installed	

RISK MANAGEMENT PLAN / STRATEGY

Description	
Specialized Security Services, Inc. identified that the new Risk Management Plan is in draft stages and at a high level. S3 recommends that the plan continue to be built out to include a method for tracking of vulnerabilities to conclusion, Supply Chain Risk Management concepts, identifying roles and responsibilities for Privacy issues, requiring contractors to adhere to Corporate policies, and record retention parameters.	
Key Activities & Prerequisites	
Sub Initiatives	Prerequisites
Track vulnerabilities to closure: Ensure that all risk assessment, penetration test, and vulnerability scan findings result in a ticket with an assigned owner to track to closure.	N/A
Supply Chain Risk Management: Evaluate the [Client]'s IT supply chain and implement safeguards and risk mitigation strategies in the event of supply chain disruption.	List of IT Vendors
Privacy: Identify dedicated resources from IT and Cybersecurity to coordinate with Legal or other departments on privacy issues.	N/A
Contract employees sign adherence to Corporate policies: Require that contractors agree to adhere to corporate policies.	N/A
Record Retention schedule: Identify and document appropriate record retention periods for IT documentation.	Corporate Retention Schedule

	Q4 2024	Q1 2025	Q2 2025	Q3 2025	Q4 2025
TIMELINE					

CONFIDENTIAL; NOT FOR DISTRIBUTION

Key Stakeholder Group	
Business Units / IT Security / IT	
Prioritization	
Maturity Impact	Low
Risk Reduction	Low
Est. Level of Effort	Medium
Sample Operational Metrics	
# of contractors that have signed policies - Record Retention Schedule published - Supply Chain identified - Reporting of risk metrics to executive leadership	

23

YOUR CYBERSECURITY PARTNER



S|3 SPECIALIZED SECURITY SERVICES

FLOAT ON

Cybersecurity and compliance to ward off any threat.

Wherever You Are in Your Cybersecurity Journey—We're With You

At S3 Security, we meet you where you are—whether you're just beginning to assess risk or advancing a mature security program. We understand the complexities you face, and we know that one of the greatest benefits of strong compliance and cybersecurity practices is lasting peace of mind.

Our mission is to strengthen your organization's resilience, efficiency, and long-term success by aligning security strategies with your business goals.

With decades of experience guiding clients through evolving regulatory requirements and emerging threats, we are your trusted partner in navigating the ever-changing technology and compliance landscape.

CONTACT US

SPECIALIZED SECURITY SERVICES, INC.

4975 Preston Park Blvd., Suite 510

Plano, TX 75093

972-378-5554 | info@s3security.com

www.s3security.com