YourIT!
Your Logo Goes Here

NIST CSF Assessment

NIST CSF Risk Report Update

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

NIST CSF Risk Report Overview

The NIST CSF Risk Report aggregates risk analysis from multiple assessments performed on the network, providing you with both a NIST CSF Risk Score and a high-level overview of the health and security of the network.

The report details the scan tasks undertaken to discover security issues. In addition to the overall NIST CSF Risk Score, the report also presents separate risk scores for all IT assessments (Network, Security) performed on the network environment. This includes a summary of individual issues, as well as their severity and weighting within the risk analysis.

At the end of the report, you can find a summary of the assets discovered on the network, in addition to other useful information organized by assessment type.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

NIST CSF Discovery Tasks

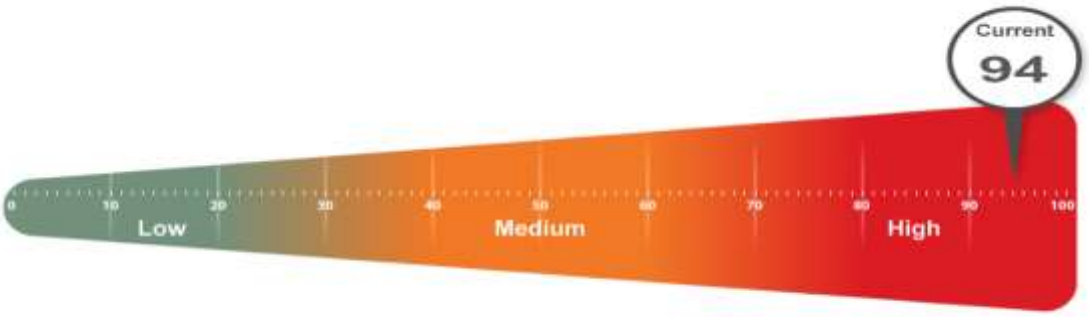
The following discovery tasks were performed.

	Task	Description
Network		
✓	Detect Domain Controllers	Identifies domain controllers and online status.
✓	FSMO Role Analysis	Enumerates FSMO roles at the site.
✓	Enumerate Organization Units and Security Groups	Lists the organizational units and security groups (with members).
✓	User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
✓	Detect Local Accounts	Detects local accounts on computer endpoints.
✓	Detect Added or Removed Computers	Lists computers added or removed from the Network since the last assessment.
✓	Detect Local Mail Servers	Detects mail server(s) on the network.
✓	Detect Time Servers	Detects server(s) on the network.
✓	Discover Network Shares	Discovers the network shares by server.
✓	Detect Major Applications	Detects all major apps / versions and counts the number of installations.
✓	Detailed Domain Controller Event Log Analysis	Lists the event log entries from the past 24 hours for the directory service, DNS server and file replication service event logs.
✓	Web Server Discovery and Identification	Lists the web servers and type.
✓	Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
✓	Internet Access and Speed Test	Tests Internet access and performance.
✓	SQL Server Analysis	Lists the SQL Servers and associated database(s).
✘	Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.
✓	Missing Security Updates.	Identifies computers missing security updates.
✓	System by System Event Log Analysis	Discovers the five system and app event log errors for servers.
✓	External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.
Security		
✓	Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
✓	Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
✓	Detect User Controls	Determines if controls are in place for user web browsing.
✘	Detect Wireless Access	Detects and determines if wireless networks are available and secured.

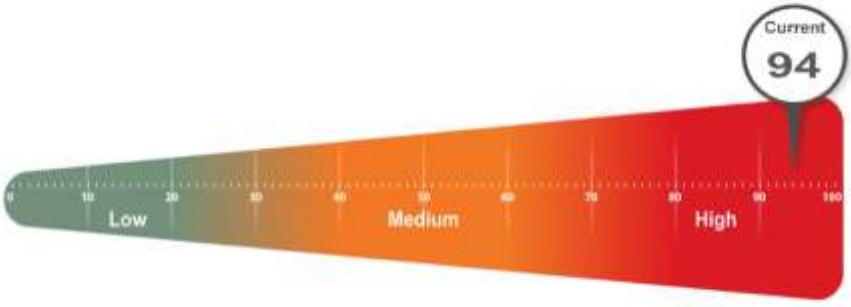
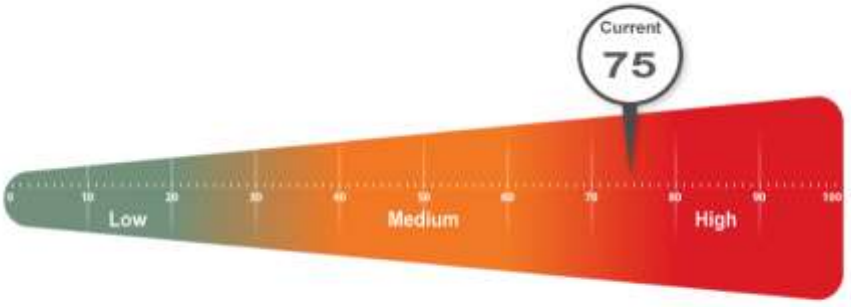
	Task	Description
✓	External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and categorizes external security threats.
✓	Network Share Permissions	Documents access to file system shares.
✓	Domain Security Policy	Documents domain computer and domain controller security policies.
✓	Local Security Policy	Documents and assesses consistency of local security policies.

Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



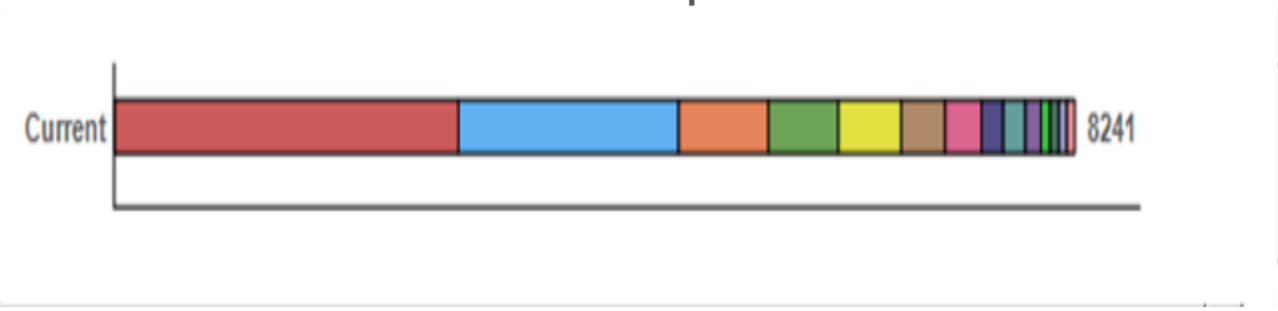
Several critical issues were identified. Identified issues should be investigated and addressed according to the NIST CSF Risk Report.

Issue Type	Risk Score
Network	
Security	

Issue Graph

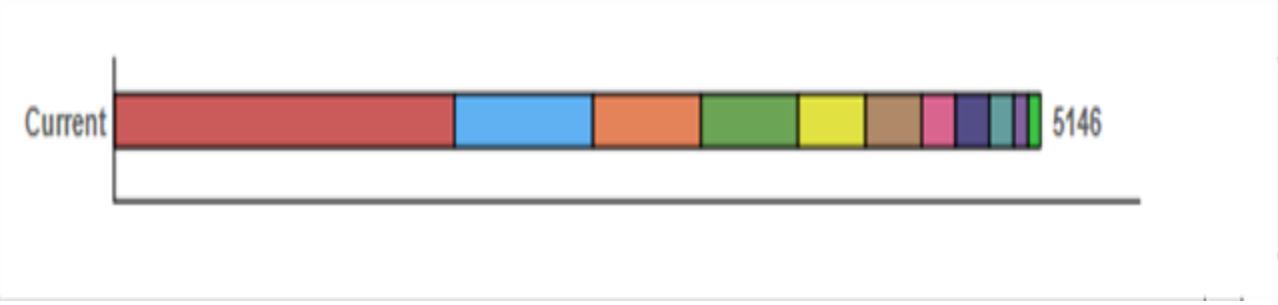
This section contains a summary of issues detected during the NIST CSF Assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.

Issue Graph

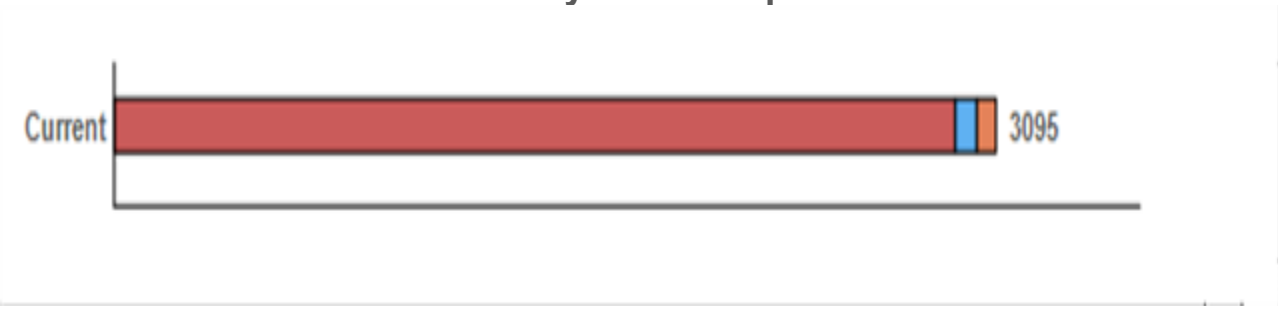


Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

Network Issue Graph



Security Issue Graph



Issue Summary

Network Issue Summary

	Anti-spyware not up to date (90pts each)
1890	***Current Score:*** 90pts x21 = 1890: 36.73%
	Issue: Up to date anti-spyware definitions are required to properly prevent the spread of malicious software. Some anti-spyware definitions were found to not be up to date.
	Recommendation: Ensure anti-spyware definitions are up to date on specified computers.

	Significantly high number of Domain Administrators (35pts each)
770	***Current Score:*** 35pts x22 = 770: 14.96%
	Issue: More than 30% of the users are in the Domain Administrator group and have unfettered access to files and system resources. Compromised Domain Administrator accounts pose a higher threat than typical users and may lead to a breach.
	Recommendation: Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary.

	User password set to never expire (30pts each)
600	***Current Score:*** 30pts x20 = 600: 11.66%
	Issue: User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.
	Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

	Anti-virus not up to date (90pts each)
540	***Current Score:*** 90pts x6 = 540: 10.49%
	Issue: Up to date anti-virus definitions are required to properly prevent the spread of malicious software. Some anti-virus definitions were found to not be up to date.
	Recommendation: Ensure anti-virus definitions are up to date on specified computers.

	Few Security patches missing on computers. (75pts each)
375	***Current Score:*** 75pts x5 = 375: 7.29%
	Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Few is defined as missing 3 or less patches.
	Recommendation: Address patching on computers missing 1-3 security patches.

	User has not logged on to domain in 30 days (13pts each)
312	***Current Score:*** 13pts x24 = 312: 6.06%

	Issue: Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.
	Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

	Anti-virus not installed (94pts each)
188	***Current Score:*** 94pts x2 = 188: 3.65%
	Issue: Anti-virus software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: To prevent both security and productivity issues, we strongly recommend ensuring that anti-virus is deployed to all possible endpoints.

	Anti-spyware not installed (94pts each)
188	***Current Score:*** 94pts x2 = 188: 3.65%
	Issue: Anti-spyware software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: Assure that anti-spyware is deployed to all possible endpoints in order to prevent both security and productivity issues.

	Inactive computers (15pts each)
135	***Current Score:*** 15pts x9 = 135: 2.62%
	Issue: Computers have not checked in during the past 30 days.
	Recommendation: Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, logged into by authorized users, or powered on.

	Operating system in Extended Support (20pts each)
80	***Current Score:*** 20pts x4 = 80: 1.55%
	Issue: Computers are using an operating system that is in Extended Supported. Extended Support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.
	Recommendation: Upgrade computers that have operating systems in Extended Support before end of life.

	Potential disk space issue (68pts each)
68	***Current Score:*** 68pts x1 = 68: 1.32%
	Issue: 1 computer were found with significantly low free disk space.
	Recommendation: Free or add additional disk space for the specified drives.

Security Issue Summary

	Automatic screen lock not turned on. (72pts each)
2952	***Current Score:*** 72pts x41 = 2952: 95.38%
	Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.
	Recommendation: Enable automatic screen lock on the specified computers.

	Medium severity external vulnerabilities detected (75pts each)
75	***Current Score:*** 75pts x1 = 75: 2.42%
	Issue: Medium severity external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
	Recommendation: Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.

	Inconsistent password policy / Exceptions to password policy (68pts each)
68	***Current Score:*** 68pts x1 = 68: 2.2%
	Issue: Password policies are not consistently applied from one computer to the next. A consistent password policy ensure adherence to password best practices.
	Recommendation: Eliminate inconsistencies and exceptions to the password policy.