YourIT!
Your Logo Goes Here

NIST CSF Assessment

NIST CSF Risk Treatment Plan

Prepared for:
Your Client's Company
Prepared by:
YourIT Company

Table of Contents

1 - Network Management Plan

2 - Security Management Plan

3 - NIST Risk Treatment Plan

Network Management Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

Risk Score	Recommendation	Severity	Probability
90	Ensure anti-virus definitions are up to date on specified computers. ☐ Computer: SQLSVR02 IP Address: 176.16.1.21 Security Center: Windows Defender ☐ Computer: WRKSTN7-2 IP Address: 176.16.1.115 Security Center: Windows Defender ☐ Computer: WRKSTN7-1 IP Address: 176.16.1.111 Security Center: Windows Defender	H	H
90	Ensure anti-spyware definitions are up to date on specified computers. ☐ Computer: WRKSTN10-4 IP Address: 176.16.1.114 Security Center: Windows Defender ☐ Computer: SQLSVR02 IP Address: 176.16.1.21 Security Center: Windows Defender	H	H
75	Address patching on computers missing 1-3 security patches. ☐ WRKSTN7-2 / fe80::846b:496b:a90e:a968%10,176.16.1.115 / Windows 7 Professional	M	H

Low Risk

Risk Score	Recommendation	Severity	Probability
35	Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary. ☐ abadmin / A Branaugh ☐ ajadmin / A Smith ☐ Administrator / Administrator ☐ dadmin / D Brown	L	M

Risk Score	Recommendation	Severity	Probability
	☐ dkadmin / D Kindle ☐ dwadmin / D White ☐ jsadmin / J Shearing ☐ jwadmin / J Westerfield ☐ lwadmin / L Wilson ☐ mgadmin / M Green ☐ mpadmin / M Peters ☐ msadmin / M Simpson ☐ pkadmin / P Kettering ☐ psadmin / P Sulu ☐ skadmin / S Kulynee ☐ thadmin / T Harris ☐ uadmin / unitbdr admin ☐ wpadmin / W Paulson		
30	Investigate all accounts with passwords set to never expire and configure them to expire regularly. ☐ MYCLIENTSNETWORK.COM\dadmin / D Brown ☐ MYCLIENTSNETWORK.COM\dkadmin / D Kindle ☐ MYCLIENTSNETWORK.COM\jsadmin / J Shearing ☐ MYCLIENTSNETWORK.COM\jwadmin / J Westerfield ☐ MYCLIENTSNETWORK.COM\lwadmin / L Wilson ☐ MYCLIENTSNETWORK.COM\mgadmin / M Green ☐ MYCLIENTSNETWORK.COM\mpadmin / M Peters ☐ MYCLIENTSNETWORK.COM\pkadmin / P Kettering ☐ MYCLIENTSNETWORK.COM\thadmin / T Harris ☐ MYCLIENTSNETWORK.COM\ajadmin / A Smith ☐ MYCLIENTSNETWORK.COM\dwadmin / D White ☐ MYCLIENTSNETWORK.COM\mptest / M Talman ☐ MYCLIENTSNETWORK.COM\msadmin / M Simpson ☐ MYCLIENTSNETWORK.COM\psadmin / P Sulu ☐ MYCLIENTSNETWORK.COM\uadmin / unitbdr admin ☐ MYCLIENTSNETWORK.COM\wpadmin / W Paulson	L	L
20	Upgrade computers that have operating systems in Extended Support before end of life. ☐ WRKSTN8-2 / fe80::f0c9:65f9:de7f:b966%3,176.16.1.103 / Windows 8.1 Pro ☐ WRKSTN8-3 / fe80::c85c:9edf:4397:9a11%3,176.16.1.107 / Windows 8.1 Pro ☐ WRKSTN8-4 / 176.16.1.110 / Windows 8.1 Pro ☐ WRKSTN8-1 / 176.16.1.105 / Windows 8.1 Pro ☐ WRKSTN7-2 / fe80::846b:496b:a90e:a968%10,176.16.1.115 / Windows 7 Professional ☐ WRKSTN7-1 /	L	L

Risk Score	Recommendation	Severity	Probability
	fe80::4168:4b42:c98d:5ad1%10,176.16.1.111 / Windows 7 Professional		
15	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. ☐ BDR01 / / Windows Server 2016 Standard ☐ HVSVR1 / 176.16.1.11 / Windows Server 2016 Standard	L	L
13	Disable or remove user accounts for users that have not logged on to active directory in 30 days. ☐ ajadmin / A Smith ☐ arogers / Aaron Rogers ☐ Administrator / Administrator ☐ dwadmin / D White ☐ ebland / Eric Bland ☐ jkristian / Jabez Kristian ☐ jashter / Jacob Ashter ☐ jgross / Janet Gross ☐ jknight / Janet Knight ☐ jcole / Jerry Coleman ☐ jcamps / John Camps ☐ jdejesus / Jone DeJesus ☐ msadmin / M Simpson ☐ mjones / Marley Jones ☐ mptest / M Talman ☐ pwysocki / Pat Wysocki ☐ psadmin / P Sulu ☐ sjames / Stan James ☐ tshields / Tin Shields ☐ uadmin / unitbdr admin ☐ wpadmin / W Paulson	L	L

Security Management Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

Risk Score	Recommendation	Severity	Probability
77	Enable account lockout for all users.	H	H
75	Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed. ☐ Name: OpenSSH auth2-gss.c User Enumeration Vulnerability (Windows) / CVSS: 5 / IP: 97.72.92.49 ☐ Name: OpenSSH sftp-server Security Bypass Vulnerability (Windows) / CVSS: 5 / IP: 97.72.92.49 ☐ Name: OpenSSH User Enumeration Vulnerability-Aug18 (Windows) / CVSS: 5 / IP: 97.72.92.49	H	H
72	Enable automatic screen lock on the specified computers. ☐ APPSVR01 ☐ DCTLR01 ☐ DCTLR02 ☐ DESKPC-09UPSPO ☐ DESKPC-191IJQL ☐ DESKPC-35EGQCC ☐ DESKPC-4171AR0 ☐ DESKPC-534MS45 ☐ DESKPC-85BJGJT ☐ DESKPC-BDJFFLG ☐ DESKPC-F6CKERQ ☐ DESKPC-HN95P9Q ☐ DESKPC-LIFRCFU ☐ DESKPC-MJOD0L9 ☐ DESKPC-QFC42PE ☐ DESKPC-RB3LBP3 ☐ DESKPC-U1K3NAF ☐ EXCHSVR01 ☐ FILESVR01 ☐ SQLSVR01 ☐ WRKSTN10-1 ☐ WRKSTN10-2 ☐ WRKSTN10-3 ☐ WRKSTN10-4	M	M

Risk Score	Recommendation	Severity	Probability
	☐ WRKSTN7-1 ☐ WRKSTN7-2 ☐ WRKSTN8-2 ☐ WRKSTN8-3		

NIST Risk Treatment Plan

This ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

[redacted] High Risk

Risk Score	Recommendation	Severity	Probability
100	**RS.IM-2: Response strategies are updated** Ensure response strategies are reviewed and updated at least every 90 days.	H	H
100	**ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders ID.RM-2: Organizational risk tolerance is determined and clearly expressed ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis** Define a Risk Management Strategy that meets the criteria set forth in ID.RM and include it in the organization's Cybersecurity Policies and Procedures.	H	H
100	**ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed** Ensure that legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are not understood and managed.	H	H
100	**DE.AE-3: Event data are collected and correlated from multiple sources and sensors** Collect and correlate event data from multiple sources and sensors.	H	H
100	**DE.AE-4: Impact of events is determined** Determine the impact of events.	H	H
100	**DE.AE-5: Incident alert thresholds are established**	H	H

Risk Score	Recommendation	Severity	Probability
	Establish incident alert thresholds.		
100	**DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability** Clearly define and document roles and responsibilities for detection to ensure accountability.	H	H
100	**DE.DP-2: Detection activities comply with all applicable requirements** Ensure detection activities comply with all applicable requirements.	H	H
100	**DE.DP-4: Event detection information is communicated** Communicate event detection information to relevant stakeholders.	H	H
100	**DE.DP-5: Detection processes are continuously improved** Continuously improve detection processes.	H	H
100	**ID.AM-3: Organizational communication and data flows are mapped** Document and map organizational communication and data flows.	H	H
100	**ID.BE-1: The organization's role in the supply chain is identified and communicated** Identify the organization's role in the supply chain and communicate it to key stakeholders.	H	H
100	**ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated** Identify organization's place in critical infrastructure and its industry sector and communicate it to key stakeholders.	H	H
100	**ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated** Establish priorities for organizational mission, objectives, and activities and communicate it to key stakeholders.	H	H
100	**ID.BE-4: Dependencies and critical functions for delivery of critical services are established** Establish dependencies and critical functions for delivery of critical services.	H	H
100	**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)**	H	H

Risk Score	Recommendation	Severity	Probability
	Establish dependencies and critical functions for delivery of critical services.		
100	**ID.GV-1: Organizational cybersecurity policy is established and communicated** Establish and communicate organizational cybersecurity policy.	H	H
100	**RS.IM-1: Response plans incorporate lessons learned** Ensure response plans incorporate lessons learned.	H	H
100	**ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.** Have contracts with suppliers and third-party partners reviewed by a qualified professional, such as a lawyer, to ensure they meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	H	H
100	**PR.DS-5: Protections against data leaks are implemented** Deploy firewalls between the internal network and all externally facing network connections.	H	H
100	**PR.DS-4: Adequate capacity to ensure availability is maintained** Deploy a monitoring system to ensure adequate disk and storage is available to ensure data availability.	H	H
100	**ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders** Establish cyber supply chain risk management processes that are assessed, managed, and agreed to by organizational stakeholders.	H	H
100	**ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.** Assess suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	H	H
100	**ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers** Conduct response and recovery planning and testing with suppliers and third-party providers	H	H

Risk Score	Recommendation	Severity	Probability
100	**PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes** Establish a documented process to issue, manage, verify, revoke and audit identities and credentials.	H	H
100	**PR.AC-2: Physical access to assets is managed and protected** Address deficiencies found in how physical access to assets are managed and protected.	H	H
100	**PR.AC-3: Remote access is managed** Establish a system to manage remote access.	H	H
100	**PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)** Protect network integrity through network segregation, network segmentation, or another means.	H	H
100	**PR.AT-1: All users are informed and trained** Ensure all users receive cybersecurity awareness education and training as part of their on-boarding and on a routine basis.	H	H
100	**PR.AT-2: Privileged users understand their roles and responsibilities** Ensure privileged users receive enhanced cybersecurity awareness education and training describing their roles and responsibilities.	H	H
100	**PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities** Communicate to third-party stakeholders their roles and responsibilities with regards to cybersecurity.	H	H
100	**PR.AT-4: Senior executives understand their roles and responsibilities** Ensure senior executives receive enhanced cybersecurity awareness education and training describing their roles and responsibilities.	H	H
100	**PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities** Ensure physical and cybersecurity personnel receive enhanced cybersecurity awareness education and training describing their roles and responsibilities.	H	H

Risk Score	Recommendation	Severity	Probability
100	**PR.DS-1: Data-at-rest is protected** Establish and document a methodology to protect data-at-rest.	H	H
100	**PR.DS-2: Data-in-transit is protected** Establish and document a methodology to protect data-in-transit.	H	H
100	**PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition** Establish and document a methodology to formally manage assets throughout removal, transfers, and disposition.	H	H
100	**ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners** Coordinated and align cybersecurity roles and responsibilities with internal roles and external partners.	H	H
100	**PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity** Employ integrity checking mechanisms to verify software, firmware, and information integrity.	H	H
100	**PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities** Incorporate the principle of least functionality by configuring systems to provide only essential capabilities.	H	H
100	**PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access** Approve, log, and perform remote maintenance of organizational assets in a manner that prevents unauthorized access	H	H
100	**PR.PT-2: Removable media is protected and its use restricted according to policy** Protect removable media and restrict its use according to policy.	H	H
100	**PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy** Determine, document, implement, and review audit/log records in accordance with policy.	H	H
100	**PR.IP-1: A baseline configuration of information**	H	H

Risk Score	Recommendation	Severity	Probability
	technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) Create and maintain a baseline configuration of information technology/industrial control systems incorporating security principles (e.g. concept of least functionality)		
100	**PR.IP-2: A System Development Life Cycle to manage systems is implemented** Implement a System Development Life Cycle to manage systems.	H	H
100	**PR.IP-3: Configuration change control processes are in place** Implement and document configuration change control processes.	H	H
100	**PR.IP-4: Backups of information are conducted, maintained, and tested** Ensure backups of information are not conducted, maintained, and tested.	H	H
100	**PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met** Ensure policy and regulations regarding the physical operating environment for organizational assets are met.	H	H
100	**PR.IP-6: Data is destroyed according to policy** Ensure data is not destroyed according to policy.	H	H
100	**PR.IP-7: Protection processes are improved** Implement a policy and procedure to ensure protection processes are regularly reviewed and improved.	H	H
100	**DE.AE-2: Detected events are analyzed to understand attack targets and methods** Analyze detected events to understand attack targets and methods.	H	H
100	**PR.IP-8: Effectiveness of protection technologies is shared** Implement a policy and procedure to ensure the effectiveness of protection technologies is shared.	H	H
100	**PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed**	H	H

Risk Score	Recommendation	Severity	Probability
	Put in place and manage response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery).		
100	**PR.IP-10: Response and recovery plans are tested** Regularly test response and recovery plans.	H	H
100	**PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)** Include cybersecurity in human resources practices (e.g., deprovisioning, personnel screening).	H	H
100	**PR.IP-12: A vulnerability management plan is developed and implemented** Develop and implement a vulnerability management plan.	H	H
100	**PR.DS-7: The development and testing environment(s) are separate from the production environment** Ensure the development and testing environment(s) are separated from the production environment.	H	H
100	**PR.PT-4: Communications and control networks are protected** Protect communications and control networks.	H	H
100	**RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks** Ensure newly identified vulnerabilities are mitigated or documented as accepted risks.	H	H
100	**RS.RP-1: Response plan is executed during or after an incident** Document in writing response plan to be executed during and after a cybersecurity incident.	H	H
100	**PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity** Employ integrity checking mechanisms to verify hardware integrity.	H	H
100	**PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations** Implement mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	H	H
100	**RC.IM-1: Recovery plans incorporate lessons learned**	H	H

Risk Score	Recommendation	Severity	Probability
	Ensure recovery plans incorporate lessons learned.		
100	**RC.IM-2: Recovery strategies are updated** Ensure recovery strategies are reviewed and updated at least every 90 days.	H	H
100	**RC.CO-2: Reputation is repaired after an incident** As part of the recovery strategy, put in place a program to repair reputation both internally and externally	H	H
100	**RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams** Ensure recovery activities are communicated to internal and external stakeholders as well as executive and management teams.	H	H
100	**RS.CO-1: Personnel know their roles and order of operations when a response is needed** Ensure personnel know their roles and order of operations when a response is needed.	H	H
100	**RS.MI-1: Incidents are contained** Ensure cybersecurity incidents are contained.	H	H
100	**RS.CO-2: Incidents are reported consistent with established criteria** Ensure incidents are reported consistent with established criteria.	H	H
100	**RS.CO-3: Information is shared consistent with response plans** Ensure incident response information is shared consistent with response plan.	H	H
100	**RS.CO-4: Coordination with stakeholders occurs consistent with response plans** Ensure coordination with stakeholders occurs consistent with response plans.	H	H
100	**RS.AN-1: Notifications from detection systems are investigated** Ensure notifications from detection systems are investigated.	H	H
100	**RS.AN-3: Forensics are performed** Ensure forensics are performed in response to a cybersecurity incident.	H	H

Risk Score	Recommendation	Severity	Probability
100	**RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)** Ensure processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).	H	H
100	**PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools** Perform and log maintenance and repair of organizational assets with approved and controlled tools	H	H
90	**PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions** Ensure authentication is required for critical applications and external systems or a compensating control is in place to mitigate the risk. ☐ etrigue	H	H
80	**ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established** Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners).	H	H

Low Risk

Risk Score	Recommendation	Severity	Probability
20	**RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness** Share information with external stakeholders to achieve broader cybersecurity situational awareness.	L	L