{customer}

Cybersecurity Gap Assessment Report

Table of Contents

Introduction

TPx conducted a Cybersecurity Gap Assessment on behalf of {customer}. This engagement was designed to evaluate {customer}'s security program in a variety of areas, with the goal of providing {customer} with a summary of (a) their current ability to defend their organization against cyberthreats; (b) their ability to maintain a level cyberdefense moving forward; and (c) a list of actionable items that they can perform to increase their security posture and reduce overall risk to the organization. The primary TPx Consultants for the assessment were {consultant 1} and {consultant 2}.

This document serves as the contract Deliverable *Cybersecurity Gap Assessment Report*, as specified in the Statement of Work outlining the work scope for this engagement. It provides the results of the detailed investigation into the customer's security environment, as well as a list of recommended next steps for {customer} to undertake to further mature their security footprint.

Documents Provided

The following documents are the contract deliverables for the gap assessment.

{customer} - Gap Assessment Heatmap.pdf

Provides a "heatmap" of the NIST 800-171 standards that are applicable to gap assessments. Each item is rated on a scale of 0 to 5 as indicated above.

{customer} - Gap Assessment Interviews.pdf

Lists questions and responses received during interviews conducted to obtain additional information or clarification.

This document is in the same sequence as the heatmap.

{customer} - Gap Assessment Project.pdf

Documents the project status.

{customer} - Gap Assessment Report.pdf

Contains the complete results of the gap assessment, including statistics, recommendations, and for each topic in the heatmap: rating, findings, best practices, and recommendations.

This document is in the same sequence as the heatmap.

{customer} - Gap Assessment Summary.pdf

Provides a high-level Executive Summary of the results of the Gap Assessment.

Heatmap Summary

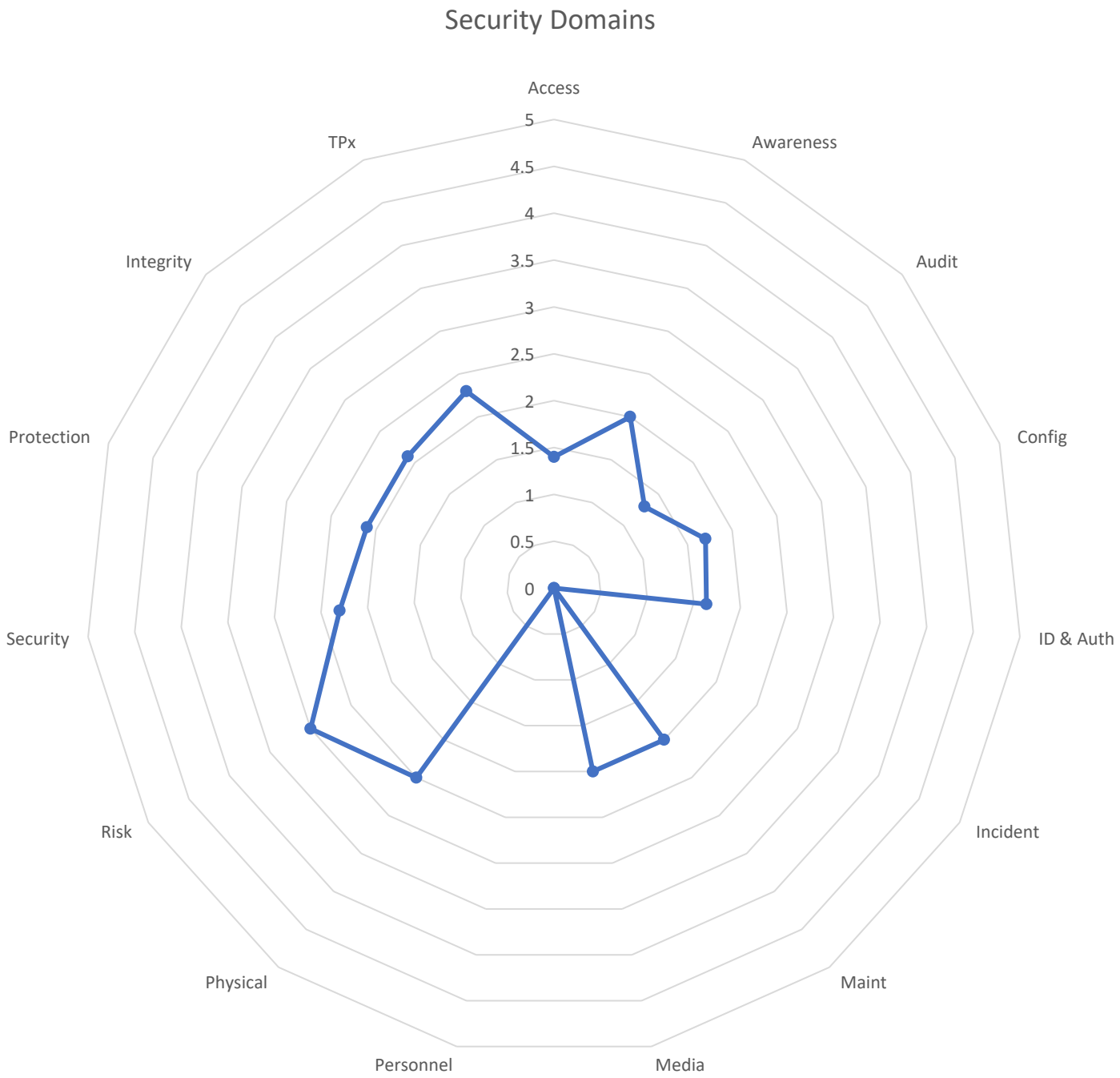
Overall Security Program Score

(2) - Developing

Developing information security requirements, practices, controls and/or documentation that translate into repeatable results.

Security Domain Ratings

Security Domains	Assessor Rating	Target Level	Risk Gap
Access Control	1.4	5	-3.6
Awareness and Training	2.0	5	-3.0
Audit and Accountability	1.3	5	-3.7
Configuration Management	1.7	5	-3.3
Identification and Authentication	1.6	5	-3.4
Incident response	0.0	5	-5.0
Maintenance	2.0	5	-3.0
Media Protection	2.0	5	-3.0
Personnel Security	0.0	5	-5.0
Physical Protection	2.5	5	-2.5
Risk Assessment	3.0	5	-2.0
Security Assessment	2.3	5	-2.7
System and Communications Protection	2.1	5	-2.9
System and Information Integrity	2.1	5	-2.9
TPx	2.3	5	-2.7
	1.8	5	-3.2


Security Domains
Access
Awareness
Audit
Config
ID & Auth
Incident
Maint
Media
Personnel
Physical
Risk
Security
Protection
Integrity
TPx
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0

Recommendations

This section lists TPx recommendations for items where shortcomings or vulnerabilities were identified.

Notes:

- High-Priority Recommendations lists highest priority recommendations.
- Summary Recommendations are listed by category:
    - General: Recommendations of a global nature.
    - Formalize and document: Recommendations to formalize policies, procedures, or processes and to document them.
    - Document: Recommendations to document existing policies, procedures, or processes.
    - Access security: Recommendations regarding access security.
    - Network security: Recommendations regarding network security.
    - Data security: Recommendations regarding data security.
    - Workstation security: Recommendations regarding workstation security.
- Recommendations also appear in the section Assessment Results.

High-Priority Recommendations

NIST Domain(s)	Description
3.13.1 3.13.2	Emails are not a secure method for transmitting passwords. Consider alternate methods of providing passwords such as sealed envelope, token, encrypted email, Microsoft Teams, etc.
3.1.6 3.2.7	Wherever possible, replace common IT user id and password with individual user ids and passwords so actions can be traced back to individuals. Document any areas or systems where that is not possible and why.
3.7.4	Implement MFA wherever possible, including VPN and remote network access.
	Migrate to WIFI 6 security as soon as humanly possible.
	Establish and document encryption policy and procedures for mobile devices, including laptops, tablets, smart phones, and any other mobile computing system (laptops are already encrypted, but it's not documented).

Summary Recommendations

This section lists recommendations by category.

General

- Create and maintain an inventory of hardware and software assets, including subscriptions for cloud-based applications.
- Establish and document audit reporting procedures.
- Establish and document controls for identifying, reporting, and correcting system flaws.

Formalize and Document

- Establish and document policy for correcting deficiencies in organizational systems.
- Establish and document Script development standards, including coding, testing, and deployment
- Establish and document a vulnerability remediation policy, including how VM snapshots are used for rollback in the event of issues with updates.
- Establish and document a vulnerability scanning policy.
- Establish and document mobile device encryption policy and procedures.
- Establish and document an asset review policy where inventory of hardware and software assets are reviewed to plan for assets approaching end-of-life or end-of support.
- Establish and document policy on how end-of-life or end-of-support hardware and software assets are to be deprecated and disposed of. Ensure disposal company is compliant with policy.
- Include peripherals (printers, scanners, etc.) in monitoring, control, and security policies, as well as end-of-life and end-of-support policies.

Document

- Document DR testing procedures and execute full DR test at least annually.
- Add simplified network diagram and data flows to existing documentation.
- Document how alerts are configured, how they should be managed and used, and how they should be addressed.
- Document how network and endpoints are protected.
- Document how network and endpoints are monitored and how alerts are addressed.
- Document how blacklisting/whitelisting is configured in firewall policies.
- Document how encryption is used with both data and communications.
- Document how functions are segregated via access controls and permissions, using least privilege principles.
- Document how least functionality principle is used and implemented.
- Document how geographic locks are configured and used.
- Document how internal system clocks are synchronized.
- Document tools, reports, and alerts used to monitor accesses, and how they should be used.
- Document which tools can be used to monitor organizational systems, and how to use them.

- Document anti-malware patching in {document reference}. Security Patching.
- Include list of authorized software in {document reference}.

Access Security

- Emails are not a secure method for transmitting passwords. Consider alternate methods of providing passwords such as sealed envelope, token, encrypted email, or via Microsoft Teams etc.
- Wherever possible, replace common IT user id and password with individual user ids and passwords so actions can be traced back to individuals. Document any areas or systems where that is not possible and why.
- Obscure feedback of authentication information.
- Review logged events regularly to identify potential discrepancies.
- Implementing timed logoff (auto logoff after a certain amount of time has passed), not just for applications, but also for computers and network sessions).
- Document how user identifiers are used, including if they can be re-used, when they are disabled or deleted, etc.
- Document how logon attempts are restricted (number of attempts, wait times between retries, when account is locked, etc.)
- Document what temporary user ids are, when they should be used, when they are disabled, etc.

Network Security

- Implement MFA wherever possible, including VPN and remote network access.
- Migrate to WIFI 6 as soon as possible to increase WIFI security.
- Document DLP configuration.
- Document firewall configuration.
- Document how VLANs are segregated.
- Document how subnetworks are defined and used.
- Document how remote access routing is managed.

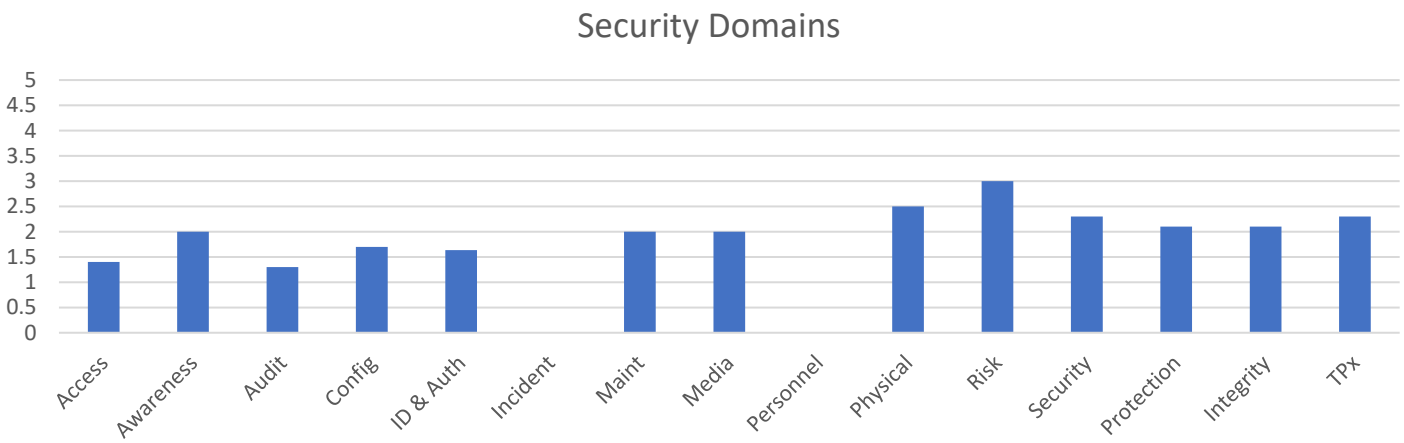
Data Security

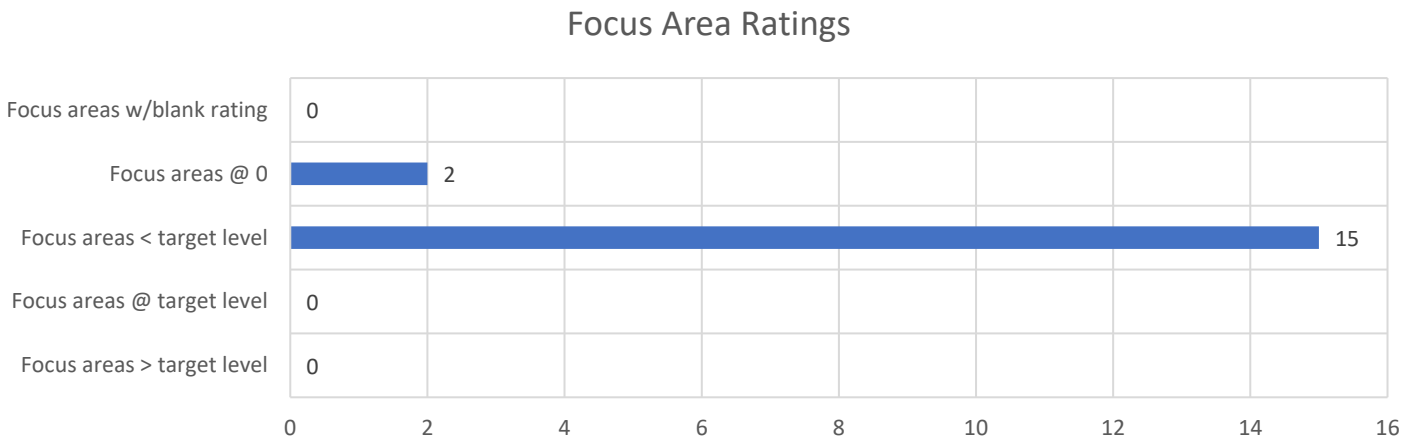
- Establish and document encryption policy and procedures for mobile devices, including laptops, tablets, smart phones, and any other mobile computing system (laptops are already encrypted, just need to document that fact).
- Establish and document controls to ensure only IT can manage audit logging functionality.
- Establish and document regular security control assessments.
- Establish and document regular security control monitoring.
- Establish and document how changes should be reviewed to determine potential security impact, and how changes should be rolled back in the event of issues.

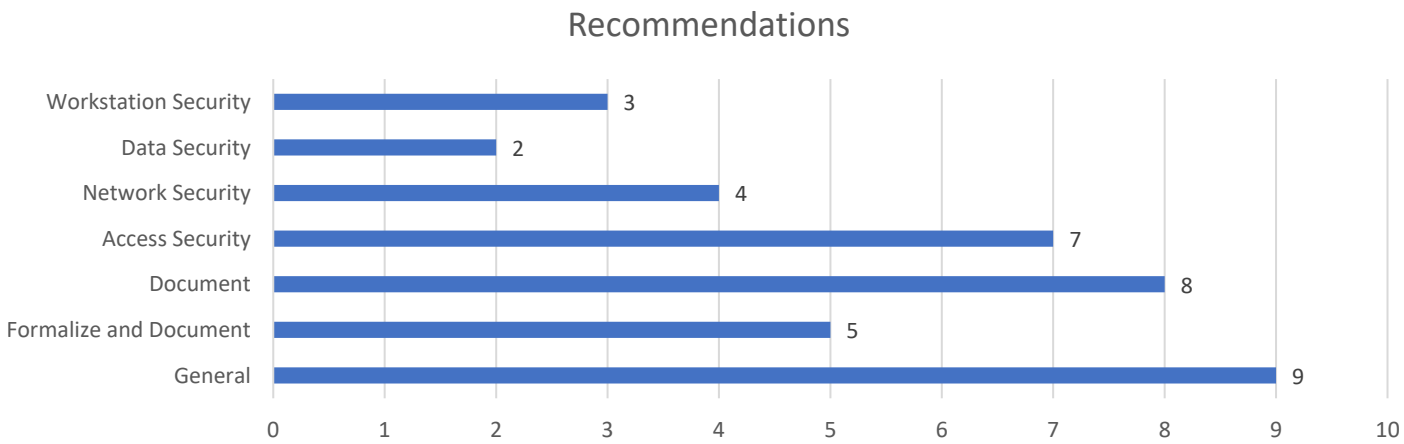
Workstation Security

- Document and enforce session auto lock.
- Document auto-logoff standards for both computers and applications.
- Document users account lockdown policy.
- Document how non-essential programs, functions, ports, protocols, and/or services are managed.
- Document how application blacklisting is configured and works, and what happens if users attempt to use blacklisted applications.

Statistics


Security Domains
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
Access
Awareness
Audit
Config
ID & Auth
Incident
Maint
Media
Personnel
Physical
Risk
Security
Protection
Integrity
TPx


Focus Area Ratings
Focus areas w/blank rating
0
Focus areas @ 0
2
Focus areas < target level
15
Focus areas @ target level
0
Focus areas > target level
0
0
2
4
6
8
10
12
14
16


Recommendations
Workstation Security
3
Data Security
2
Network Security
4
Access Security
7
Document
8
Formalize and Document
5
General
9
0
1
2
3
4
5
6
7
8
9
10

Assessment Results

Based on the review of {customer}'s documentation and interviews, the target level was set to 5.0 for all NIST items reviewed, with one exception: NIST 3.13.2 (target was set at 3.0).

Findings are listed in the same sequence as the heatmap.

Access Control

NIST 3.1.1 - Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Rated	4/5
Findings	MFA used for O365 & ConnectWise Automate. No indication of MFA used for VPN or network access. Biometrics are allowed, but not enforced.
Best Practices	Make use of MFA to secure system access.
Recommendations	Implement MFA wherever possible, including VPN and remote network access.

NIST 3.1.2 - Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Rated	4/5
Findings	Admin functions segregated via access controls and permissions, using least privilege principles. Not documented, but in place. Tools, reports, and alerts used to monitor accesses and determine access changes needed.
Best Practices	Use least privilege principles and segregate access based on user function(s).
Recommendations	Document how functions are segregated via access controls and permissions, using least privilege principles. Document tools, reports, and alerts used to monitor accesses.

NIST 3.1.3 - Control the flow of CUI in accordance with approved authorizations.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.1.4 - Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Rated	4/5
Findings	Users account lockdown policy in place. No separation of individual duty in the vein of "Personnel responsible".
Best Practices	Use groups and/or profiles to limit functionality based on user's role.
Recommendations	Document users account lockdown policy.

NIST 3.1.5 - Employ the principle of least privilege, including for specific security functions and privileged accounts.

Rated	3/5
Findings	IT uses a common user id and password only known to IT team.
Best Practices	Use individual user ids and passwords whenever possible so actions can be traced by to individuals.
Recommendations	Wherever possible, replace common IT user id and password with individual user ids and passwords so actions can be traced back to individuals. Document any areas or systems where that is not possible and why.

NIST 3.1.6 - Use non-privileged accounts or roles when accessing nonsecurity functions

Rated	4/5
Findings	Admin functions segregated via access controls and permissions, using least privilege principles. Not documented, but in place. Tools, reports, and alerts used to monitor accesses and determine access changes needed.
Best Practices	Use least privilege principles and segregate access based on user function(s).
Recommendations	Document how functions are segregated via access controls and permissions, using least privilege principles.

NIST 3.1.7 - Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Rated	3/5
Findings	ConnectWise Automate used to monitor processes and sessions.
Best Practices	Use technology (firewalls, system tools, audit logs, etc.) to detect and prevent unauthorized access.
Recommendations	Document tools, reports, and alerts used to monitor accesses.

NIST 3.1.8 - Limit unsuccessful logon attempts.

Rated	4/5
Findings	Unsuccessful logon attempts are limited to 5 attempts, followed by a 30-minute wait. If the user retries within 10 minutes, the account is locked.
Best Practices	Limit number of attempts and lock user accounts if the limit is exceeded.
Recommendations	Document how logon attempts are restricted (number of attempts, wait times between retries, when account is locked, etc.)

NIST 3.1.9 - Provide privacy and security notices consistent with applicable CUI rules.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.1.10 - Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity

Rated	4/5
Findings	Session auto-lock after 5 minutes of inactivity.
Best Practices	Lock sessions after a pre-determined amount of time and use a screen saver or an image to hide screen content.
Recommendations	Document and enforce session auto lock standards.

NIST 3.1.11 - Terminate (automatically) a user session after a defined condition.

Rated	3/5
Findings	No auto logoff on PCs, but applications have auto logoff.
Best Practices	Logoff computers and applications when they have been unused for a pre-determined amount of time.
Recommendations	Implement timed logoff (auto logoff after a certain amount of time has passed), not just for applications, but also for computers and network sessions. Document any new auto-logoff standards as well as any existing ones.

NIST 3.1.12 - Monitor and control remote access sessions.

Rated	4/5
Findings	80% of employees have remote access by logging via VPN. Remote users are placed in separate VLAN. They can access production servers, but not other VLANs. Sessions are recorded and geo-locked to region. All PCs connecting are required to be domain joined. And those that are not have access revoked.
Best Practices	Use technology (firewalls, VPNs, MFA, etc.) to help detect, prevent, and remediate remote access attacks.
Recommendations	Document tools, reports, and alerts used to monitor accesses, and how they should be used. Document how VLANs are segregated. Document how geographic locks are configured and used.

NIST 3.1.13 - Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Rated	4/5
Findings	All data at rest is encrypted. Encryption across WAN via Cisco routers (256 bit AES). Kerberos across environment layer 6 encryption, VPN encryption via SSL certification 2048 bit. WIFI using WPA-2 personal, looking to upgrade to security features in WIFI 6.
Best Practices	Use strong encryption to protect data and communications.
Recommendations	Document how encryption is used with both data and communications.

NIST 3.1.14 - Route remote access via managed access control points.

Rated	4/5
Findings	Remote access routing via firewall and VPN, however this is not documented.
Best Practices	Use technology (firewalls, VPNs, MFA, etc.) for remote access routing.
Recommendations	Document how remote access routing is managed.

NIST 3.1.15 - Authorize remote execution of privileged commands and remote access to security-relevant information.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.1.16 - Authorize wireless access prior to allowing such connections

Rated	3/5
Findings	Currently using WPA-2 Personal for WIFI access. Migration to WIFI 6 planned.
Best Practices	Use strong security protocols for wireless access.
Recommendations	Migrate to WIFI 6 security as soon as humanly possible.

NIST 3.1.17 - Protect wireless access using authentication and encryption

Rated	3/5
Findings	Currently using WPA-2 Personal for WIFI access. Migration to WIFI 6 planned.
Best Practices	Use strong security protocols for wireless access.
Recommendations	Migrate to WIFI 6 security as soon as humanly possible.

NIST 3.1.18 - Control connection of mobile devices.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.1.19 - Encrypt CUI on mobile devices and mobile computing platforms.[23]

Rated	0/5
Findings	Laptops are encrypted, but there’s no indication of encryption of other mobile devices.
Best Practices	Encrypt mobile devices to secure data they contain.

Recommendations	Create new policy for mobile device encryption, including laptops, tablets, smart phones, and any other mobile computing system.

NIST 3.1.20 - Verify and control/limit connections to and use of external systems.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.1.21 - Limit use of portable storage devices on external systems.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.1.22 - Control CUI posted or processed on publicly accessible systems.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

Awareness and Training

NIST 3.2.1 - Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

Rated	5/5
Findings	Detailed overview of phishing available in {document reference}. Limited mention of other attack vectors. Security Awareness Training is yet to be rolled out to the full extent. Quickhelp.com security training is available to all personnel.
Best Practices	Provide documentation and training on security risks and how to mitigate them.
Recommendations	None.

NIST 3.2.2 - Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.2.3 - Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

Audit and Accountability

NIST 3.3.1 - Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity

Rated	5/5
Findings	All data is to remain on systems unless otherwise instructed for the use of audit logging and data retention.
Best Practices	Create and store system audit logs and records.
Recommendations	None.

NIST 3.3.2 - Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

Rated	5/5
Findings	Employees are forbidden from tampering with audit trails (deletion of browsing history is emphasized).
Best Practices	Ensure actions can be traced by to individual users.
Recommendations	None.

NIST 3.3.3 - Review and update logged events.

Rated	5/5
Findings	Assess events as they come in. Have endpoint protection that sends alerts on a regular basis. Events are categorized based upon criticality.
Best Practices	Logged events should be regularly reviewed.
Recommendations	Document how alerts are configured, how they should be managed and used, and how they should be addressed. Review logged events regularly to identify potential discrepancies.

NIST 3.3.4 - Alert in the event of an audit logging process failure.

Rated	3/5
Findings	No documented alerting process outlined; however, subject matter experts are made aware of events via endpoint management system.
Best Practices	Implement alerts for audit logging process failure.
Recommendations	Document how alerts are configured, how they should be managed and used, and how they should be addressed.

NIST 3.3.5 - Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

Rated	5/5
Findings	Employees are forbidden from tampering with audit trails (deletion of browsing history is emphasized). Subject Matter Experts confirmed that deletion of any internal materials hosted on local environment is strictly forbidden.
Best Practices	Define and document process for reviewing audit and event logs.
Recommendations	None.

NIST 3.3.6 - Provide audit record reduction and report generation to support on- demand analysis and reporting.

Rated	2/5
Findings	No mention of audit reporting or report generation in either documentation or attestation. Subject matter experts had no knowledge of this capability.
Best Practices	Establish and document audit reporting procedures.
Recommendations	Define and document audit reporting procedures.

NIST 3.3.7 - Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Rated	3/5
Findings	Not documented. However, verbally confirmed that internal clocks are synced.
Best Practices	Configure system clocks to synchronize with authoritative source.
Recommendations	Document how internal system clocks are synchronized.

NIST 3.3.8 - Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Rated	5/5
Findings	All data at rest is encrypted. Encryption across WAN via Cisco routers (256-bit AES). Kerberos across environment layer 6 encryption, VPN encryption via SSL certification 2048 bit. WIFI using WPA-2 personal, looking to upgrade to security features in WIFI 6.
Best Practices	Protect audit data and tools with user access rights and encryption.
Recommendations	Document how encryption is used with both data and communications.

NIST 3.3.9 - Limit management of audit logging functionality to a subset of privileged users.

Rated	5/5
Findings	Only IT personnel have this functionality
Best Practices	Limit management of audit logging functionality to IT personnel.
Recommendations	Establish and document controls to ensure only IT has this functionality.

Configuration Management

NIST 3.4.1 - Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Rated	5/5
Findings	{document reference}.
Best Practices	Establish and maintain baseline configurations and inventories of organizational systems throughout system development life cycles.
Recommendations	None.

NIST 3.4.2 - Establish and enforce security configuration settings for information technology products employed in organizational systems.

Rated	5/5
Findings	{document reference}.
Best Practices	Establish and enforce security configuration settings for information technology products
Recommendations	None.

NIST 3.4.3 - Track, review, approve or disapprove, and log changes to organizational systems.

Rated	5/5
Findings	{document reference}.
Best Practices	Define and document procedures for tracking, reviewing, approving, and logging changes.
Recommendations	None.

NIST 3.4.4 - Analyze the security impact of changes prior to implementation.

Rated	1/5
Findings	No plan in place. Ensured that changes can be backed up in event of failure. Changes are made outside hours of operation.
Best Practices	Define and document process for analyzing security impact of changes.
Recommendations	Establish and document how changes should be reviewed to determine potential security impact, and how changes should be rolled back in the event of issues.

NIST 3.4.5 - Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

Rated	5/5
Findings	Clearly defined throughout {document reference}.
Best Practices	Define and document access restrictions associated with changes.
Recommendations	None.

NIST 3.4.6 - Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

Rated	3/5
Findings	Default domain policy. Principle of least functionality is not documented.
Best Practices	Define and document how least functionality principle is used and implemented.
Recommendations	Document how least functionality principle is used and implemented.

NIST 3.4.7 - Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

Rated	4/5
Findings	Admin functions segregated via access controls and permissions, using least privilege principles. Not documented, but in place. Tools, reports, and alerts used to monitor accesses and determine access changes needed. IT uses a common local user/password only known to IT team.
Best Practices	Disable any non-essential programs, functions, ports, protocols, and/or services.
Recommendations	Document how non-essential programs, functions, ports, protocols, and/or services are managed.

NIST 3.4.8 - Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.4.9 - Control and monitor user-installed software.

Rated	4/5
Findings	Defined within {document reference}. Lacks documented listing of user-installed software.
Best Practices	Block users from being able to install software.
Recommendations	Include list of authorized software in {document reference}.

Identification and Authentication

NIST 3.5.1 - Identify system users, processes acting on behalf of users, and devices.

Rated	4/5
Findings	ConnectWise Automate used to monitor processes and sessions. Blacklisted applications will generate alerts if a user attempts to use them.
Best Practices	Use technology to monitor user activity and raise alerts.
Recommendations	Document tools, reports, and alerts used to monitor accesses. Document how application blacklisting is configured and works, and what happens if users attempt to use blacklisted applications.

NIST 3.5.2 - Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Rated	4/5
Findings	Palo Alto Firewall monitoring internal & external boundaries. ConnectWise Automate used to monitor processes and sessions. Tools, reports, and alerts used to monitor accesses. MFA used for O365 & ConnectWise Automate. No indication of MFA used for VPN or network access.
Best Practices	Use strong user verification technologies to ensure secure access.
Recommendations	Implement MFA wherever possible, including VPN and remote network access.

NIST 3.5.3 - Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.[24] [25].

Rated	4/5
Findings	MFA used on all O365 access and ConnectWise Automate. Biometrics being considered (Windows Hello). Currently implementing Bitdefender Password Vault with MFA. No indication of MFA used for VPN or network access.
Best Practices	Use MFA for user verification.
Recommendations	Implement MFA wherever possible, including VPN and remote network access.

NIST 3.5.4 - Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Rated	4/5
Findings	Identifiers are not re-used.
Best Practices	Do not allow re-use of user identifiers.
Recommendations	Document how user identifiers are used, including if they can be re-used, when they are disabled or deleted, etc.

NIST 3.5.5 - Prevent reuse of identifiers for a defined period.

Rated	4/5
Findings	Identifiers are not re-used.
Best Practices	Do not allow re-use of user identifiers.
Recommendations	Document how user identifiers are used, including if they can be re-used, when they are disabled or deleted, etc.

NIST 3.5.6 - Disable identifiers after a defined period of inactivity.

Rated	4/5
Findings	Unused user identifiers are disabled.
Best Practices	Disable identifiers when they have not been used for a predetermined amount of time.
Recommendations	Document how user identifiers are used, including if they can be re-used, when they are disabled or deleted, etc.

NIST 3.5.7 - Enforce a minimum password complexity and change of characters when new passwords are created.

Rated	5/5
Findings	{document reference}.
Best Practices	Establish strong password policy.
Recommendations	None.

NIST 3.5.8 - Prohibit password reuse for a specified number of generations.

Rated	5/5
Findings	Retention is currently set at 24 generations.
Best Practices	Do not allow passwords from being re-used for a predetermined amount of time.
Recommendations	None.

NIST 3.5.9 - Allow temporary password use for system logons with an immediate change to a permanent password.

Rated	5/5
Findings	Temporary user ids are enabled only temporarily and are disabled when associated tasks are completed. Generally used for external vendors.
Best Practices	Allow temporary passwords but require user to change them at first use.
Recommendations	None.

NIST 3.5.10 - Store and transmit only cryptographically protected passwords.

Rated	3/5
Findings	New passwords are sent to users via standard email and they are required to change them at their next logon.
Best Practices	Passwords should always be communicated using encrypted means.
Recommendations	Emails are not a secure method for transmitting passwords. Consider alternate methods of providing passwords such as encrypted email, sealed envelope, token, etc.

NIST 3.5.11 - Obscure feedback of authentication information.

Rated	4/5
Findings	No indication that feedback of authentication information is obscured.
Best Practices	Obscure feedback of authentication information.
Recommendations	Obscure feedback of authentication information.

Incident response

NIST 3.6.1 - Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Rated	5/5
Findings	Covered in {document reference}.
Best Practices	Operational incident policies and procedures need to be well documented and be readily available to appropriate staff.
Recommendations	None.

NIST 3.6.2 - Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Rated	5/5
Findings	Covered in {document reference}.
Best Practices	Incident tracking, documenting, and reporting policies need to be well documented and be readily available to appropriate staff.
Recommendations	None.

NIST 3.6.3 - Test the organizational incident response capability.

Rated	3/5
Findings	Last full DR test was in 2018. BDR tested annually, but not as a full failover test (tests connections and sub-applications work ok). Full failover test schedule for in 30+ days. VMs are replicated to DR site. Health monitoring on replication. Replicated VMs tested every 90 days.
Best Practices	Disaster recovery (DR) testing policy should be documented and should include full DR tests at least annually.
Recommendations	Document DR testing procedures and execute full DR test.

Maintenance

NIST 3.7.1 - Perform maintenance on organizational systems.[26].

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated

Recommendations	Not evaluated

NIST 3.7.2 - Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.7.3 - Ensure equipment removed for off-site maintenance is sanitized of any CUI.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.7.4 - Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.7.5 - Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.7.6 - Supervise the maintenance activities of maintenance personnel without required access authorization.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

Media Protection

NIST 3.8.1 - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.8.2 - Limit access to CUI on system media to authorized users

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.8.3 - Sanitize or destroy system media containing CUI before disposal or release for reuse.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.8.4 - Mark media with necessary CUI markings and distribution limitations.[27]

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated

Recommendations	Not evaluated

NIST 3.8.5 - Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.8.6 - Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.8.7 - Control the use of removable media on system components.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.8.9 - Protect the confidentiality of backup CUI at storage locations.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

Personnel Security

NIST 3.9.1 - Screen individuals prior to authorizing access to organizational systems containing CUI.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.9.2 - Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

Rated	5/5
Findings	{document reference}. {contact} stated there have no departures since joining.
Best Practices	Ensure sensitive data is protected
Recommendations	None.

Physical Protection

NIST 3.10.1 - Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.10.2 - Protect and monitor the physical facility and support infrastructure for organizational systems.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.10.3 - Escort visitors and monitor visitor activity.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.10.4 - Maintain audit logs of physical access.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.10.5 - Control and manage physical access devices.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.10.6 - Enforce safeguarding measures for CUI at alternate work sites.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

Risk Assessment

NIST 3.11.1 - Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated

Recommendations	Not evaluated

NIST 3.11.2 - Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Rated	3/5
Findings	{document reference}. Vulnerability policy outlined, however not routinely deployed.
Best Practices	Schedule periodic vulnerability scans.
Recommendations	Establish and document a vulnerability scanning policy.

NIST 3.11.3 - Remediate vulnerabilities in accordance with risk assessments.

Rated	3/5
Findings	Not documented. Using VM snapshots for rollback of deployment if issues with update.
Best Practices	Remediate vulnerabilities as they are identified.
Recommendations	Establish and document a vulnerability remediation policy, including how VM snapshots are used for rollback in the event of issues with updates.

Security Assessment

NIST 3.12.1 - Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Rated	3/5
Findings	Plan is not formally written down. There are periodic assessments. Not consistent.
Best Practices	Regularly assess security controls.
Recommendations	Establish and document regular security control assessments.

NIST 3.12.2 - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Rated	1/5
Findings	No plans identified. {document} document addressed security gaps but no official plan to develop POA&M.
Best Practices	Have a well-defined plan of action to correct deficiencies in organizational systems.

Recommendations	Develop and implement plan of action to correct deficiencies in organizational systems.

NIST 3.12.3 - Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Rated	1/5
Findings	Note present in policy or procedure
Best Practices	Establish policy for ongoing security control monitoring.
Recommendations	Establish and document regular security control monitoring.

NIST 3.12.4 - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Rated	4/5
Findings	Network diagram has been outlined, however, lack security functionality description.
Best Practices	Create and document system security plan.
Recommendations	Add simplified network diagram and data flows to existing documentation.

System and Communications Protection

NIST 3.13.1 - Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Rated	4/5
Findings	Using WPA-2 Personal for WIFI access. Migration to WIFI 6 planned.
Best Practices	Use firewall Unified Threat Management (UTM) features to increase network security
Recommendations	Migrate to WIFI 6 security as soon as humanly possible.

NIST 3.13.2 - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Rated:	2/3
Findings	No inhouse software development other than scripts, but no formal process. Adjustments are made to legacy systems when appropriate.

Best Practices	Any development should follow established and documented standards, even script development. This can include development and testing standards, configuration management, code blocks (header blocks, change logs, user input handling, error handling, etc.), etc.
Recommendations	Define and document script coding standards, including coding, testing, and deployment.

NIST 3.13.3 - Separate user functionality from system management functionality.

Rated:	3/5
Findings	Admin functions segregated via access controls and permissions, using least privilege principles. Not documented, but in place. Tools and reports used to monitor accesses and determine access changes needed. IT uses a common user ID and password only known to IT team.
Best Practices	Use of least privilege principles is good, but it should be documented. The use of common user ids and passwords is not recommended because actions performed cannot always be traced back to those who executed them.
Recommendations	Document how functions are segregated via access controls and permissions, using least privilege principles. Document tools, reports, and alerts used to monitor accesses. Wherever possible, replace common IT user id and password with individual user ids and passwords so actions can be traced back to individuals. Document any areas or systems where that is not possible and why.

NIST 3.13.4 - Prevent unauthorized and unintended information transfer via shared system resources.

Rated	5/5
Findings	DLP enabled on Palo Alto. Notification for any large uploads or data exfiltration. Daily report plus real time alerts. Did not find references to use of DLP in documentation.
Best Practices	Prevent data loss using Data Loss Prevention (DLP) on firewalls and activating related alerts. Prevent authorized or unintended data transfer via shared system resources.
Recommendations	Document DLP configuration.

NIST 3.13.5 - Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Rated	5/5
Findings	Public network segregated internally (VLAN) and traffic coming in (isolated machine).

Best Practices	Publicly accessible system components should be physically or logically separated from internal networks using separate LANs or isolated VLANs.
Recommendations	Document how subnetworks are defined and used.

NIST 3.13.6 - Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Rated	4/5
Findings	Using WPA-2 Personal for WIFI access. Migration to WIFI 6 planned.
Best Practices	Use firewall Unified Threat Management (UTM) features to increase network security.
Recommendations	Migrate to WIFI 6 security as soon as humanly possible.

NIST 3.13.7 - Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

Rated	5/5
Findings	Blocked at firewall level. Only domain joined devices can connect to the network.
Best Practices	Constrain remote devices from establishing connections to organizational systems using firewalls, VPNs, and Multi-Factor Authentication.
Recommendations	Document firewall configuration.

NIST 3.13.8 - Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.13.9 - Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.13.10 - Establish and manage cryptographic keys for cryptography employed in organizational systems.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.13.11 - Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.13.12 - Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29].

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.13.13 - Control and monitor the use of mobile code.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.13.14 - Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.13.15 - Protect the authenticity of communications sessions.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

NIST 3.13.16 - Protect the confidentiality of CUI at rest.

Rated:	0/5
Findings	Not evaluated
Best Practices	Not evaluated
Recommendations	Not evaluated

System and Information Integrity

NIST 3.14.1 Identify, report, and correct system flaws in a timely manner.

Rated	3/5
Findings	Outage policy in place. Nothing formally written down in regard to a management matrix.
Best Practices	Define and implement a process to identify, report, and correct system flaws.
Recommendations	Establish and document controls for identifying, reporting, and correcting system flaws.

NIST 3.14.2 Provide protection from malicious code at designated locations within organizational systems.

Rated	5/5
Findings	Endpoint protection covers. No documented procedure.
Best Practices	Provide protection from malicious code at firewall and endpoints.
Recommendations	Document how network and endpoints are protected.

NIST 3.14.3 Monitor system security alerts and advisories and take action in response.

Rated	5/5
Findings	Endpoint protection covers. No documented procedure.
Best Practices	Monitor and respond to system alerts and advisories.

Recommendations	Document how network and endpoints are monitored and how alerts are addressed.

NIST 3.14.4 Update malicious code protection mechanisms when new releases are available.

Rated	4/5
Findings	{document reference}. Need clarification for antimalware patching capabilities. Article 8 "Security Patching" does not mention antimalware patching.
Best Practices	Define and document anti-malware patching.
Recommendations	Document anti-malware patching in {document}, paragraph {paragraph}.

NIST 3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Rated	5/5
Findings	{document reference}
Best Practices	Schedule periodic scans, and scan files from external sources as they are downloaded, opened, or executed.
Recommendations	None.

NIST 3.14.6 - Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Rated	5/5
Findings	Monitoring capabilities allow visibility into all traffic across the network. Automatic blacklisting in the event of unauthorized application use.
Best Practices	Monitor systems to detect attacks and Indicators of Compromise.
Recommendations	Document which tools can be used to monitor organizational systems, and how to use them.

NIST 3.14.7 - Identify unauthorized use of organizational systems.

Rated	4/5
Findings	Palo Alto Firewall monitoring internal & external boundaries. ConnectWise Automate used to monitor processes and sessions. Tools, reports, and alerts used to monitor accesses.
Best Practices	Use technology (firewalls, VPNs, MFA, etc.) to help detect, prevent, and remediate unauthorized access.
Recommendations	Document tools, reports, and alerts used to monitor accesses.

TPx

TPx 1.1 - Establish and maintain a list of all licensed hardware and software assets utilized by the organization, including subscriptions for cloud-based offerings.

Rated	0/5
Findings	No mention in IT Asset Disposal Policy.
Best Practices	Maintain a list of hardware and software assets, including cloud-based subscriptions.
Recommendations	Create and maintain an inventory of hardware and software assets, including subscriptions for cloud-based applications.

TPx 1.2 - Periodically review and update the list of all licensed hardware and software assets for upcoming end-of-life/end-of-support dates.

Rated	0/5
Findings	No mention in IT Asset Disposal Policy.
Best Practices	Schedule regular reviews of hardware and software assets for upcoming end-of-life and end-of-support.
Recommendations	Establish and document an asset review policy where inventory of hardware and software assets are reviewed to plan for assets approaching end-of-life or end-of support.

TPx 1.3 - Establish and enforce deprecation of end-of-life/end-of-support hardware and software assets according to dispensations guidelines regarding data disposal.

Rated	3/5
Findings	Asset disposal company is planning to handle dispensation of EoL hardware.
Best Practices	Establish policy for the deprecation of end-of-life and end-of-support hardware and software assets.
Recommendations	Establish, document, and enforce policy on how end-of-life or end-of-support hardware and software assets are to be deprecated and disposed of. Ensure disposal company is compliant with policy.

TPx 1.4 - Include printers, scanners, 3D printers, and other peripherals in all IT monitoring, control, and security.

Rated	0/5
Findings	List not included in provided documentation.
Best Practices	Include peripherals (printers, scanners, etc.) in monitoring, control, and security.

Recommendations	Include peripherals in monitoring, control, and security policies, as well as end-of-life and end-of-support policies.

Appendix A - Methodology

TPx reviewed {customer}'s security program through interviews, policy review, validation, and investigation of processes. For each focus area, the relevant policy & process documents were read and evaluated based on thoroughness, clarity, applicability to task, and alignment with National Institute of Standards and Technology (NIST) standards. Follow-up questions were then developed where necessary, and the relevant points of contact were interviewed to provide clarity and further information to the material covered in the document(s). Where possible, the technical implementation of the baseline controls was also observed and evaluated, providing insight into the execution of the defined security policies and processes.

Following the steps above, each subcomponent within a given focus area was rated on a zero to five scale with respect to the criteria outlined above. The six ratings levels are as follows:

- **Maintaining (5)** Managed information security whereby generated metrics are applied to the performance evaluation and continuous improvement of information security.
- **Managed (4)** Defined information security established that generates relevant, measurable, and useful metrics.
- **Documented (3)** Well-established information security requirements, practices, controls, and documentation that translate into consistent repeatable and predictable results.
- **Developing (2)** Developing information security requirements, practices, controls and/or documentation that translate into repeatable results.
- **Minimal (1)** Early reactive information security requirements, practices, inadequately controlled and/or documented.
- **None (0)** No information security requirements, practices, controls, or documentation.

These ratings are then aggregated across all subcomponents within each focus area, to compute an area-level rating. Finally, the area-level ratings are aggregated to provide a program-wide rating that takes into account all aspects of the customer's security program that were within the work scope of the engagement.

In each case, the subcomponent is also assigned a "target" rating level. This target represents the desired level of maturity for that subcomponent. While a 100% secure environment is desirable, it is also unattainable, due to usability, technical, budget, and other considerations. These target levels reflect the appropriate trade-off between security and these considerations, as determined for the specific environment under assessment. The difference between the target level and observed level for any subcomponent, focus area, or program, represents the "gap" between the observed and desired states.

The ratings and target levels for each subcomponent and focus area are contained in a heatmap document that accompanies this report. The heatmap enables quick identification of the subcomponents and focus areas with the largest deviation from target, and which therefore are the most likely candidates for improvement. The report included in this document contains focus area ratings and supporting narrative for each area.

For this engagement, focus areas assessed followed the NIST 800-171 security domains:

- Access Control

- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

However, the following NIST control points were excluded and were not evaluated:

- NIST 3.1.3 - Control the flow of CUI in accordance with approved authorizations.
- NIST 3.1.9 - Provide privacy and security notices consistent with applicable CUI rules.
- NIST 3.1.15 - Authorize remote execution of privileged commands and remote access to security-relevant information.
- NIST 3.1.18 - Control connection of mobile devices.
- NIST 3.1.20 - Verify and control/limit connections to and use of external systems.
- NIST 3.1.21 - Limit use of portable storage devices on external systems.
- NIST 3.1.22 - Control CUI posted or processed on publicly accessible systems.
- NIST 3.2.2 - Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
- NIST 3.2.3 - Provide security awareness training on recognizing and reporting potential indicators of insider threat.
- NIST 3.4.8 - Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- NIST 3.7.1 - Perform maintenance on organizational systems.[26].
- NIST 3.7.2 - Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
- NIST 3.7.3 - Ensure equipment removed for off-site maintenance is sanitized of any CUI.
- NIST 3.7.4 - Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
- NIST 3.7.5 - Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
- NIST 3.7.6 - Supervise the maintenance activities of maintenance personnel without required access authorization.
- NIST 3.8.1 - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

- NIST 3.8.2 - Limit access to CUI on system media to authorized users
- NIST 3.8.3 - Sanitize or destroy system media containing CUI before disposal or release for reuse.
- NIST 3.8.4 - Mark media with necessary CUI markings and distribution limitations.[27]
- NIST 3.8.5 - Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- NIST 3.8.6 - Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- NIST 3.8.7 - Control the use of removable media on system components.
- NIST 3.8.9 - Protect the confidentiality of backup CUI at storage locations.
- NIST 3.9.1 - Screen individuals prior to authorizing access to organizational systems containing CUI.
- NIST 3.10.1 - Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
- NIST 3.10.2 - Protect and monitor the physical facility and support infrastructure for organizational systems.
- NIST 3.10.3 - Escort visitors and monitor visitor activity.
- NIST 3.10.4 - Maintain audit logs of physical access.
- NIST 3.10.5 - Control and manage physical access devices.
- NIST 3.10.6 - Enforce safeguarding measures for CUI at alternate work sites.
- NIST 3.11.1 - Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI
- NIST 3.13.8 - Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
- NIST 3.13.9 - Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
- NIST 3.13.10 - Establish and manage cryptographic keys for cryptography employed in organizational systems.
- NIST 3.13.11 - Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
- NIST 3.13.12 - Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29].
- NIST 3.13.13 - Control and monitor the use of mobile code.
- NIST 3.13.14 - Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
- NIST 3.13.15 - Protect the authenticity of communications sessions.
- NIST 3.13.16 - Protect the confidentiality of CUI at rest.

An additional focus area was added for topics not covered by NIST standards, including:

- Creating a list of licensed hardware and software assets, including subscriptions.
- Periodic review and update of list of licensed hardware and software assets.
- Management of end-of-life/end-of-support hardware and software assets.
- Including peripherals in IT monitoring, control, updates, and security.

Appendix B - Documents Reviewed

Focus Area	Document Name	Revision	Document Owner (if known)
Security	Document 1	08/04/2020	Employee 1
Policies	Document 2	1.3	Employee 1
Disaster Recovery	Document 3	1.3	Employee 1
Security	Document 4	1.2	Employee 1
Change Mgmt	Document 5	2.1	Employee 2
Network	Document 6		Employee 2
General	Document 7	2	Employee 2

Appendix C – Interviews Conducted

Date	Interviewees	Topic(s) Covered
03/30/2022	{customer contact 1} {customer contact 2} {customer contact 3}	Network Architecture Review Traffic Flow Backup & Disaster Recovery MPLS/VPN Service Misconfiguration or Design flaws Weak authentication or encryption protocols Centralized Authentication, Authorization, and Accounting Attack Awareness (IPS/IDS) Rogue DHCP/Client Detection Security and system support Central Monitoring/Alerting Capabilities Syslog Capabilities Host End Monitoring/Management Software Management (networking) Configuration validation capabilities EoL/EoS hardware and licensing