Your Standard

Full Assessment

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.

Scan Date: 13-May-2022

Prepared for: Acme Distribution

Prepared by: Your IT Company

15-Jun-2022

Table of Contents

01 Overview

02 Summary

03 Detailed Requirements Assessment

- DE.AE-1 - Network operations baseline
- DE.AE-2 - Analyze events
- DE.AE-3 - Data aggregation and correlation
- DE.AE-4 - Event impact
- DE.AE-5 - Incident alerts
- DE.CM-1 - Network monitoring
- DE.CM-2 - Physical environment monitoring
- DE.CM-3 - Personnel monitoring
- DE.CM-4 - Malicious code detection
- DE.CM-5 - Mobile code
- DE.CM-6 - External service provider monitoring
- DE.CM-7 - Unauthorized activity monitoring
- DE.CM-8 - Vulnerability scans
- DE.DP-1 - Detection roles and responsibilities
- DE.DP-2 - Detection compliance
- DE.DP-3 - Test detection processes
- DE.DP-4 - Communicate detections
- DE.DP-5 - Detection continuous improvement
- ID.AM-1 - Hardware inventory
- ID.AM-2 - Software and Platform Inventory
- ID.AM-3 - Data Flows
- ID.AM-4 - External Information Systems
- ID.AM-5 - Resource and Data Prioritization
- ID.AM-6 - Cybersecurity Roles and Responsibilities
- ID.BE-1 - Supply Chain Role
- ID.BE-2 - Critical Infrastructure Role
- ID.BE-3 - Priorities
- ID.BE-4 - Dependencies
- ID.BE-5 - Resilience
- ID.GV-1 - Security Policy
- ID.GV-2 - Coordination
- ID.GV-3 - Legal and regulatory requirements
- ID.GV-4 - Governance and risk management processes
- ID.RA-1 - Identify vulnerabilities
- ID.RA-2 - Information sharing forums
- ID.RA-3 - Identify threats

ID.RA-4 - Identify impacts
ID.RA-5 - Determining risk
ID.RA-6 - Risk responses
ID.RM-1 - Risk management processes
ID.RM-2 - Organizational risk tolerance
ID.RM-3 - Risk tolerance determination
PR.AC-1 - Identities and credentials
PR.AC-2 - Physical access
PR.AC-3 - Remote access
PR.AC-4 - Access permissions
PR.AC-5 - Network integrity
PR.AT-1 - Training
PR.AT-2 - Privileged users
PR.AT-3 - Third-party stakeholders
PR.AT-4 - Senior executives
PR.AT-5 - Physical and information security personnel
PR.DS-1 - Data-at-rest
PR.DS-2 - Data-in-transit
PR.DS-3 - Asset management
PR.DS-4 - Capacity
PR.DS-5 - Data leak protection
PR.DS-6 - Integrity checking
PR.DS-7 - Development & testing environments
PR.IP-1 - Baseline configurations
PR.IP-2 - System Development Life Cycle
PR.IP-3 - Configuration change control
PR.IP-4 - Backups
PR.IP-5 - Physical operating environment
PR.IP-6 - Data destruction
PR.IP-7 - Continuous improvement
PR.IP-8 - Sharing information
PR.IP-9 - Incident Response and Business Continuity Plans
PR.IP-10 - Incident response and recovery plan testing
PR.IP-11 - Human Resource practices
PR.IP-12 - Vulnerability management
PR.MA-1 - Maintenance
PR.MA-2 - Remote maintenance
PR.PT-1 - Logging & Audit Controls
PR.PT-2 - Removable media
PR.PT-3 - Least functionality
PR.PT-4 - Communications protection
RC.CO-1 - Manage public relations
RC.CO-2 - Reputation repair
RC.CO-3 - Communicate recovery activities

RC.IM-1 - Recovery lessons learned
RC.IM-2 - Update recovery strategies
RC.RP-1 - Execute recovery plan
RS.AN-1 - Investigate notifications
RS.AN-2 - Incident impact
RS.AN-3 - Perform forensics
RS.AN-4 - Categorize incidents
RS.CO-1 - Response roles and responsibilities.
RS.CO-2 - Event reporting
RS.CO-3 - Response information sharing
RS.CO-4 - Response coordination
RS.CO-5 - Voluntary information sharing
RS.IM-1 - Response lessons learned
RS.IM-2 - Update response strategies
RS.MI-1 - Contain incidents
RS.MI-2 - Mitigate incidents
RS.MI-3 - Newly identified vulnerabilities
RS.RP-1 - Execute response plans
04 Internal Controls
CC1.1 - Inventories
CC1.2 - Data Locations
CC1.3 - Data Flow Mapping
CC1.5 - Baseline Configurations
CC2.1 - Organization's Supply Chain Role
CC2.2 - Organization's Critical Infrastructure Role
CC2.4 - Workforce Cybersecurity Roles & Responsibilities
CC2.8 - Roles & Responsibilities Coordination
CC2.11 - Detection Roles & Responsibilities
CC2.12 - Privileged Users
CC2.13 - Third-Parties
CC2.14 - Senior Executives
CC2.15 - Physical Security Personnel
CC3.1 - Legal and Regulatory Requirements
CC4.1 - Written Cybersecurity Policies
CC5.1 - Risk Assessment/Risk Analysis
CC5.2 - Prioritize Risks
CC7.1 - Identity Management
CC7.2 - Physical Access Management
CC7.3 - Remote Access Management
CC7.4 - Access Permission Management
CC7.5 - Network Segregation
CC7.6 - HR Cybersecurity Alignment
CC8.1 - Protect Data

CC8.2 - Manage Assets
CC8.3 - Ensure Adequate Capacity
CC8.4 - Protect Against Data Leaks
CC8.5 - Integrity Checking
CC8.6 - Separate Development & Testing Environments
CC8.7 - Implement Life Cycle
CC8.8 - Change Controls
CC8.10 - Data Destruction
CC8.13 - Improve Processes
CC8.14 - Share Effectiveness Information
CC8.15 - Protect & Restrict Removable Media
CC8.16 - Control & Limit Access
CC8.41 - Incident Management Process
CC9.2 - Perform & Control Maintenance & Repairs
CC9.4 - Manage Remote Maintenance
CC10.1 - Implement Logging/Audit Controls
CC11.1 - Physical Access Policies
CC13.1 - In-transit Data Protection
CC13.5 - Monitor, Control, and Protect Communications
CC14.1 - Business Continuity & Disaster Recovery Plans
CC14.2 - Resource Criticality
CC14.4 - Organizational Priorities
CC14.7 - Dependencies
CC14.8 - Resliency Requirements
CC14.9 - Business Impact Analysis
CC14.10 - Likelihood Analysis
CC14.12 - Data Backup Plan
CC14.13 - Backups
CC14.15 - Restoration Testing
CC14.18 - Recovery Capability Testing
CC16.1 - Workforce Training
CC17.1 - Vulnerability Scans
CC17.2 - Vulnerability Plan
CC17.5 - Identify Threats
CC17.6 - Threat and Vulnerability Information
CC17.7 - Risk Determination
CC17.8 - Risk Responses
CC17.9 - Risk Management
CC17.10 - Risk Tolerance
CC17.11 - Risk Tolerance Alignment
CC17.12 - Newly-Identified Vulnerabilities
CC18.2 - Triage Events
CC18.6 - Event Data Correlation
CC18.7 - Event Impact Determination

CC18.8 - Incident Alert Thresholds
CC18.10 - Physical Environment Monitoring
CC18.11 - Personnel Activity Monitoring
CC18.12 - Malicious Code Detection
CC18.13 - Mobile Code Detection
CC18.14 - Monitor Service Provider Activity
CC18.15 - Monitoring
CC18.16 - Detection Compliance
CC18.17 - Test Detection Processes
CC18.18 - Detection Information Communications
CC18.19 - Improve Detection Processes
CC19.1 - Incident Response Plan
CC19.3 - Contain Incidents
CC19.4 - Mitigate Incidents
CC19.5 - Perform Forensics
CC19.6 - Categorize Incidents
CC19.7 - Understand Incident Impact
CC19.8 - Investigate Detection System Notifications
CC19.14 - Personnel Incident Responsibilities
CC19.15 - Incident Reporting Determination
CC19.16 - Incident Documentation & Reporting
CC19.17 - Incident Information Sharing
CC19.19 - Stakeholder Incident Coordination
CC19.20 - Stakeholder Information Sharing
CC19.21 - Response Plan Lessons Learned
CC19.22 - Update Response Strategies
CC20.1 - Follow Incident Recovery Plan
CC20.2 - Recovery Plan Lessons Learned
CC20.3 - Update Recovery Strategies
CC20.4 - Manage Public Relations
CC20.5 - Reputation Repair
CC20.6 - Communicate Recovery Activities

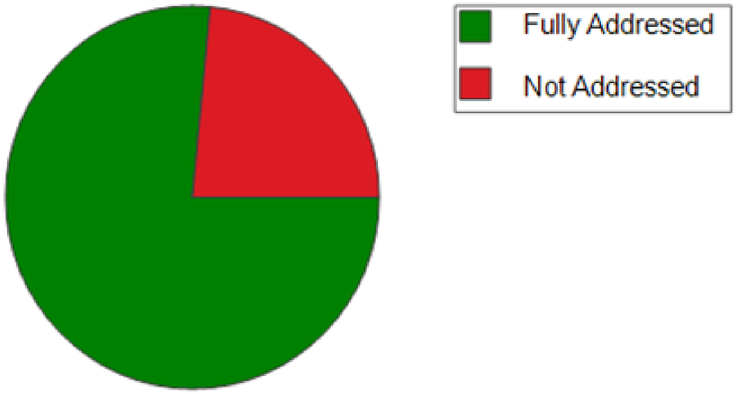
1 - Overview

We perform a periodic assessment of our information system environment with regards to the principals and functions set as part of NIST CSF. The assessment consists of automated scans in conjunction with a review by an Internal Assessor.

This document contains both direct evidence of compliance along with attestations by the Internal Assessor based on a review of materials and supporting documentation.

The methodology for the review and supporting documentation can be found in the various worksheets and documents (referenced in the NIST CSF Assessor Checklist). Issues are noted in the NIST CSF Plan of Action and Milestones. Technical Issues are noted in the Technical Risk Analysis and Technical Risk Treatment Plan.

2 - Summary



ASSESSMENT	# REQUIREMENTS
Fully Addressed	75
Not Addressed	23
Total Requirements	**98**

3 - Detailed Requirements Assessment

DE.AE-1 - Network operations baseline

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

Overall Assessment: **Addressed**

Comments:

The Security Officer develops and communicates baseline configurations and a written System Development Life Cycle to ensure that all devices and services provide an adequate level of security to meet the needs of the organization. The life cycle takes into consideration performance, security, and the needs of the organization to remain competitive in its markets.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC1.5 - Baseline Configurations	Establish and maintain baseline configurations of organizational systems (including hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, firmware, and reporting requirements) throughout the respective system development life cycles.	Fully Implemented

DE.AE-2 - Analyze events

DE.AE-2: Detected events are analyzed to understand attack targets and methods.

Overall Assessment: **Addressed**

Comments:

Response and recovery plans are executed during or after an event. Notifications from detection systems are investigated and documented. The impact of the incident is analyzed and understood. Forensics are performed and incident are categorized.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.2 - Triage Events	Analyze and triage events to support event	Fully Implemented

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
	resolution and incident declaration.	

DE.AE-3 - Data aggregation and correlation

DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors

Overall Assessment: **Addressed**

Comments:

Detected events are analyzed to understand attack targets and methods. Event data is aggregated and correlated from multiple sources and sensors. Impact of events is determined.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.6 - Event Data Correlation	Ensure that event data are aggregated and correlated from multiple sources and sensors.	Fully Implemented

DE.AE-4 - Event impact

DE.AE-4: Impact of events is determined.

Overall Assessment: **Addressed**

Comments:

Detected events are analyzed to understand attack targets and methods. Event data is aggregated and correlated from multiple sources and sensors. Impact of events is determined.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.7 - Event Impact Determination	Ensure that the impact of events is determined.	Fully Implemented

DE.AE-5 - Incident alerts

DE.AE-5: Incident alert thresholds are established.

Overall Assessment: **Addressed**

Comments:

Incident alert thresholds have been established by the Security Officer, who will review logs, either manually or through an automated process. IDS/IPS are especially helpful in identifying anomalies. Having network baselines helps rule out false positives in anomaly detection.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.8 - Incident Alert Thresholds	Ensure that incident alert thresholds are established.	Fully Implemented

DE.CM-1 - Network monitoring

DE.CM-1: The network is monitored to detect potential cybersecurity events

Overall Assessment: **Addressed**

Comments:

The Security Officer regularly reviews records associated with the monitoring of system activity to identify any patterns of activity that suggest the organization's security policies and procedures have been breached, either by members of its workforce or by outside individuals or organizations. The Security Officer determines whether security has been violated and takes appropriate corrective action, including changes in security policies and procedures.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.15 - Monitoring	Ensure that monitoring the network for unauthorized personnel, connections, devices, and software is performed.	Fully Implemented

DE.CM-2 - Physical environment monitoring

DE.CM-2: The physical environment is monitored to detect potential cybersecurity events

Overall Assessment: **Addressed**

Comments:

Incident alert thresholds have been established by the Security Officer, who will review logs, either manually or through an automated process. IDS/IPS are especially helpful in identifying anomalies. Having network baselines helps rule out false positives in anomaly detection.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.10 - Physical Environment Monitoring		Fully Implemented

DE.CM-3 - Personnel monitoring

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

Overall Assessment: **Addressed**

Comments:

Roles and responsibilities for detection are defined by the Security Officer to ensure accountability. Detection activities must comply with all applicable requirements. Processes must be tested and continuously improved.

As a part of this process, personnel activity must be monitored to detect potential cybersecurity events.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.11 - Personnel Activity Monitoring	Ensure that personnel activity is monitored to detect potential cybersecurity events.	Fully Implemented

DE.CM-4 - Malicious code detection

DE.CM-4: Malicious code is detected

Overall Assessment: **Not Addressed**

Comments:

Yes - Partially Addressed

maintaining current patch and firmware levels, using endpoint protection software, protecting the network and mobile devices with a business-class firewall running an active intrusion prevention system.

All system and security patches is installed within 2 business days of being released. This includes operating systems, application software, malware definitions, and firewall intrusion prevention updates. Critical devices such as firewalls, network switches and infrastructure hardware, computers and servers, storage devices, and other equipment must be checked every 90-days for firmware updates.

Anti-malware software is installed on all endpoint devices and servers to protect the organization and its information from attack by malicious software such as computer viruses, worms, and Trojan horses. This software must be maintained with current subscriptions and regularly updated; must be turned on; and must be installed to prevent users from disabling or removing the software.

Workforce members are instructed to not disable anti-virus software and must immediately take action to report virus infections and remove viruses from affected machines when the anti-virus software identifies an infection

After a recent periodic review of the status of anti-virus software installed on Windows computer endpoints using automated scanning and reporting tools, 32% of all computer endpoints have the automatic update functionality of the anti-virus software installed on the identified endpoints set to disabled.

This incident has been reported and corrective action is underway.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.12 - Malicious Code Detection	Ensure that malicious code is detected.	Partially Implemented

DE.CM-5 - Mobile code

DE.CM-5: Unauthorized mobile code is detected

Overall Assessment: **Addressed**

Comments:

Mobile devices are protected against malicious software (malware.)

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.13 - Mobile Code Detection	Ensure that unauthorized mobile code is detected.	Fully Implemented

DE.CM-6 - External service provider monitoring

DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.

Overall Assessment: **Addressed**

Comments:

The Security Officer and other company leaders have implemented security processes to protect against risks from external service providers. Refer to the organization's system security plan for more specific information.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.14 - Monitor Service Provider Activity	Ensure that external service provider activity is monitored to detect potential cybersecurity events.	Fully Implemented

DE.CM-7 - Unauthorized activity monitoring

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

Overall Assessment: **Addressed**

Comments:

The Security Officer regularly reviews records associated with the monitoring of system activity to identify any patterns of activity that suggest the organization's security policies and procedures have been breached, either by members of its workforce or by outside individuals or organizations. The Security Officer determines whether security has been violated and takes appropriate corrective action, including changes in security policies and procedures.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.15 - Monitoring	Ensure that monitoring the network for unauthorized personnel, connections, devices, and software is performed.	Fully Implemented

DE.CM-8 - Vulnerability scans

DE.CM-8: Vulnerability scans are performed

Overall Assessment: **Not Addressed**

Comments:

Yes - Partially

At-risk software or devices is immediately be removed or isolated to ensure that data is fully protected and that the organization maintains compliance with regulations and other requirements

Encryption status assessments are not performed by the organization at this time.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.1 - Vulnerability Scans	Scan for vulnerabilities and encryption	Partially Implemented

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
	status in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	

DE.DP-1 - Detection roles and responsibilities

DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.

Overall Assessment: **Addressed**

Comments:

Roles and responsibilities for detection are well defined by the Security Officer to ensure accountability. Detection activities must comply with all applicable requirements. Processes must be tested and continuously improved.

A baseline of network operations and expected data flows for users and systems must be established and managed.

Detected events are analyzed to understand attack targets and methods. Event data are aggregated and correlated from multiple sources and sensors. Impact of events must be determined.

Incident alert thresholds ae established by the Security Officer, who will review logs, either manually or through an automated process. IDS/IPS are especially helpful in identifying anomalies. Having network baselines helps rule out false positives in anomaly detection.

Personnel activity is monitored to detect potential cybersecurity events.

Suspected or proven event detection information is communicated to appropriate parties in time to comply with all applicable requirements.

The Security Officer and system administrators oversee the implementation of security tools and processes to detect and manage unusual or unauthorized activity.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.11 - Detection Roles & Responsibilities	Ensure that roles and responsibilities for detection are well defined to ensure accountability.	Fully Implemented

DE.DP-2 - Detection compliance

DE.DP-2: Detection activities comply with all applicable requirements.

Overall Assessment: **Addressed**

Comments:

Roles and responsibilities for detection are well defined by the Security Officer to ensure accountability. Detection activities must comply with all applicable requirements. Processes are tested and continuously improved. Periodic reviews are performed to ensure that detection activities complete with legal and regulatory requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.16 - Detection Compliance	Ensure that detection activities comply with all applicable requirements.	Fully Implemented

DE.DP-3 - Test detection processes

DE.DP-3: Detection processes are tested

Overall Assessment: **Addressed**

Comments:

Incident alert thresholds must be established by the Security Officer, who will review logs, either manually or through an automated process. As a part of this review process, detection processes are tested and verified as operational in compliance with the organization's information security and risk management plans.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.17 - Test Detection Processes	Ensure that detection processes are tested.	Fully Implemented

DE.DP-4 - Communicate detections

DE.DP-4: Event detection information is communicated to appropriate parties.

Overall Assessment: **Addressed**

Comments:

Suspected or proven event detection information is communicated to appropriate parties in time to comply with all applicable requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.18 - Detection Information Communications	Ensure that event detection information is communicated to appropriate parties.	Fully Implemented

DE.DP-5 - Detection continuous improvement

DE.DP-5: Detection processes are continuously improved.

Overall Assessment: **Addressed**

Comments:

Roles and responsibilities for detection are defined by the Security Officer to ensure accountability. Detection activities
comply with all applicable requirements. Processes are periodically tested and continuously improved.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.19 - Improve Detection Processes	Ensure that detection processes are continuously improved.	Fully Implemented

ID.AM-1 - Hardware inventory

ID.AM-1: Physical devices and systems within the organization are inventoried.

Overall Assessment: **Not Addressed**

Comments:

Hardware Inventory Procedure: The organization will utilize an automated tool to scan our network to identify assets at least each calendar quarter. Manual inventories will supplement the automated tools to document devices and systems that cannot be identified through automation.

Software Inventory Procedure: The organization will utilize an automated tool to scan our network to identify software platforms and applications at least each calendar quarter. Manual inventories will supplement the automated tools to document platforms, applications, and cloud-based applications that cannot be identified through automation.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC1.1 - Inventories	Establish and maintain inventories of organizational systems (including hardware, hardware, portable media,	Fully Implemented

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
	mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.	

ID.AM-2 - Software and Platform Inventory

ID.AM-2: Software platforms and applications within the organization are inventoried

Overall Assessment: **Not Addressed**

Comments:

Hardware Inventory Procedure: The organization will utilize an automated tool to scan our network to identify assets at least each calendar quarter. Manual inventories will supplement the automated tools to document devices and systems that cannot be identified through automation.

Software Inventory Procedure: The organization will utilize an automated tool to scan our network to identify software platforms and applications at least each calendar quarter. Manual inventories will supplement the automated tools to document platforms, applications, and cloud-based applications that cannot be identified through automation.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC1.1 - Inventories	Establish and maintain inventories of organizational systems (including hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.	Fully Implemented

ID.AM-3 - Data Flows

ID.AM-3: Organizational communication and data flows are mapped

Overall Assessment: **Not Addressed**

Comments:

Hardware Inventory Procedure: The organization will utilize an automated tool to scan our network to identify assets at least each calendar quarter. Manual inventories will supplement the automated tools to document devices and systems that cannot be identified through automation.

Software Inventory Procedure: The organization will utilize an automated tool to scan our network to identify software platforms and applications at least each calendar quarter. Manual inventories will supplement the automated tools to document platforms, applications, and cloud-based applications that cannot be identified through automation.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC1.1 - Inventories	Establish and maintain inventories of organizational systems (including hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.	Fully Implemented
CC1.2 - Data Locations	Locate and identify all organizational data, including data stored on local devices, mobile devices, servers, mass storage, portable media, and cloud platforms.	Fully Implemented
CC1.3 - Data Flow Mapping	Create a map of how data flows within and in/out of the organization.	Fully Implemented

ID.AM-4 - External Information Systems

ID.AM-4: External information systems are catalogued

Overall Assessment: **Not Addressed**

Comments:

Hardware Inventory Procedure: The organization will utilize an automated tool to scan our network to identify assets at least each calendar quarter. Manual inventories will supplement the automated tools to document devices and systems that cannot be identified through automation.

Software Inventory Procedure: The organization will utilize an automated tool to scan our network to identify software platforms and applications at least each calendar quarter. Manual inventories will supplement the automated tools to document platforms, applications, and cloud-based applications that cannot be identified through automation.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC1.1 - Inventories	Establish and maintain inventories of organizational systems (including hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.	Fully Implemented

ID.AM-5 - Resource and Data Prioritization

ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value

Overall Assessment: **Not Addressed**

Comments:

Partially Addressed

The Security Officer has implemented manual and automated processes to classify and secure the organization's resources (e.g., hardware, devices, data, and software).

To date, the criticality of workforce member access to organization systems has not been established.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC14.2 - Resource Criticality	Establish and communicate the criticality of all resources.	Partially Implemented

ID.AM-6 - Cybersecurity Roles and Responsibilities

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

Overall Assessment: **Addressed**

Comments:

Only workforce members authorized by the organization's management may access client systems, and only for authorized purposes.

Authorized workforce members must only use access control system approved by the organization to access client sites and data. Access is limited to the minimum required for the workforce members' role.

Information and Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

The organization's workforce members are required to maintain confidentiality of client information as if it was the organization's information.

Specifically,
- Workforce members will only access client sites and data using approved mechanisms.
- No protected information may be removed from client site by physical or electronic means without specific authorization by the organization's management.
- If removal is approved, client data must be encrypted before transmission or physical movement

• No information overheard or seen at customer sites may be shared for purposes other than those authorized by the organization
• Workforce members will be trained on all regulations appropriate to their work with clients
• Workforce members will be subject to all civil and criminal penalties for non-compliance with regulations required of clients

Any client information protected by federal, state, or industry regulations must be managed in accordance with those regulations.

The Security Officer will classifies each type of workforce and third-party user's role and responsibilities and define appropriate access levels and capabilities.

Exhibits:

- Security Plans of Action.pdf

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.4 - Workforce Cybersecurity Roles & Responsibilities	Establish and document cybersecurity roles and responsibilities within the workforce.	Fully Implemented

ID.BE-1 - Supply Chain Role

ID.BE-1: The organization's role in the supply chain is identified and communicated

Overall Assessment: **Addressed**

Comments:

The organization's role in the supply chain is identified and communicated. This includes the organization's position with clients, vendors, and partners.

The organization's place in critical infrastructure and its industry sector must be identified, documented, and communicated.

Priorities for the organization's mission, objectives, and activities must be established, documented, and communicated.

The Security Officer collaborates with internal and external stakeholders to ensure that critical services are identified and prioritized, and that adequate resources are dedicated to ensuring the delivery of services and resilience to disruptions and disasters.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.1 - Organization's Supply Chain Role	Identify and communicate the organization's role in the supply chain.	Fully Implemented

ID.BE-2 - Critical Infrastructure Role

ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated

Overall Assessment: **Addressed**

Comments:

The Security Officer collaborates with internal and external stakeholders to ensure that critical services are identified and prioritized, and that adequate resources are dedicated to ensuring the delivery of services and resilience to disruptions and disasters.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.2 - Organization's Critical Infrastructure Role	Identify and communicate the organization's role in critical infrastructure.	Fully Implemented

ID.BE-3 - Priorities

ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated

Overall Assessment: **Addressed**

Comments:

The organization’s place in critical infrastructure and its industry sector has been identified, documented, and communicated to all stakeholders.

On an ongoing basis, priorities for the organization’s mission, objectives, and activities are established, documented, and communicated periodically to all affected stakeholders.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC14.4 - Organizational Priorities	Establish and communicate priorities based on the organization's mission, objectives, activities, legal requirements, and regulations.	Fully Implemented

ID.BE-4 - Dependencies

ID.BE-4: Dependencies and critical functions for delivery of critical services are established

Overall Assessment: **Addressed**

Comments:

The organization’s role in the supply chain is identified and communicated. This includes the organization’s position with clients, vendors, and partners.

The organization’s place in critical infrastructure and its industry sector must be identified, documented, and communicated.

Priorities for the organization’s mission, objectives, and activities must be established, documented, and communicated.

The Security Officer collaborates with internal and external stakeholders to ensure that critical services are identified and prioritized, and verifies that adequate resources are dedicated to ensuring the delivery of services and resilience to disruptions and disasters

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC14.7 - Dependencies	Identify and document all dependencies for each critical function. Include technology, people, and facilities.	Fully Implemented

ID.BE-5 - Resilience

ID.BE-5: Resilience requirements to support delivery of critical services are established

Overall Assessment: **Addressed**

Comments:

The Security Officer collaborates with internal and external stakeholders to ensure that critical services are identified and prioritized, and that adequate resources are dedicated to ensuring the delivery of services and resilience to disruptions and disasters

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC14.8 - Resliency Requirements	Establish resilience requirements to support the delivery of critical services.	Fully Implemented

ID.GV-1 - Security Policy

ID.GV-1: Organizational information security policy is established.

Overall Assessment: **Addressed**

Comments:

The organization's security policy is reviewed by the organization’s management each year and updated as necessary. The policy and any changes must be communicated to all workforce members.

The Security Officer ensures that information security policies are established, reviewed, and updates as necessary.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC4.1 - Written Cybersecurity Policies	Write policies addressing all cybersecurity requirements.	Fully Implemented

ID.GV-2 - Coordination

ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners

Overall Assessment: **Addressed**

Comments:

The Security Officer will classifies each type of workforce and third-party user’s role and responsibilities and define appropriate access levels and capabilities.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.8 - Roles & Responsibilities Coordination	Coordinate and align information security roles & responsibilities with internal roles and external partners.	Fully Implemented

ID.GV-3 - Legal and regulatory requirements

ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

Overall Assessment: **Addressed**

Comments:

The organization uses commercially reasonable efforts to comply with all applicable laws and regulations, including:
- Federal and State Laws
- Industry Regulations
- Contracts
- Insurance Policy Requirements

Information security roles & responsibilities will be coordinated and aligned with internal roles and external partners.

Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, must be understood and managed. Governance and risk management processes will address cybersecurity risks.

The Security Officer has identified all relevant compliance requirements, classify each type of workforce and third-party user's role and responsibilities, and define appropriate access levels and capabilities. Processes will be developed to ensure compliance with all internal and external requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC3.1 - Legal and Regulatory Requirements	Identify and manage all legal and regulatory requirements.	Fully Implemented

ID.GV-4 - Governance and risk management processes

ID.GV-4: Governance and risk management processes address cybersecurity risks.

Overall Assessment: **Addressed**

Comments:

The organization conducts periodic risk analysis to evaluate the likelihood and the impact that each security threat or vulnerability might occur.

The risk analysis describes the nature and extent of the damage each threat might cause to the integrity, availability, and confidentiality of the organization's information resources.

The risk analysis identifies high-priority threats that are the focus of risk-management efforts.

Medium and low priority threats are also identified and reviewed for mitigation.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC5.2 - Prioritize Risks	Prioritize risks according to the defined risk	Fully Implemented

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
	categories, risk sources, and risk measurement criteria.	

ID.RA-1 - Identify vulnerabilities

ID.RA-1: Asset vulnerabilities are identified and documented.

Overall Assessment: **Addressed**

Comments:

The Security Officer periodically engages a qualified independent organization to conduct an accurate and thorough risk analysis that includes vulnerabilities, threats, likelihood, and impact, in accordance with all internal and external requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC5.1 - Risk Assessment/Risk Analysis	Periodically conduct an accurate and thorough assessment of the risks 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 data.	Fully Implemented

ID.RA-2 - Information sharing forums

ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources

Overall Assessment: **Addressed**

Comments:

The Security Officer has implemented the necessary processes to access and use threat and vulnerability information is received from information sharing forums and sources as part of the organization's risk analysis process.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.6 - Threat and Vulnerability Information	Receive and respond to threat and vulnerability information from information sharing forums and sources and communicate to stakeholders.	Fully Implemented

ID.RA-3 - Identify threats

ID.RA-3: Threats, both internal and external, are identified and documented.

Overall Assessment: **Addressed**

Comments:

The organization's risk analysis process identifies threats to the security of the organization's company data, including natural, human, and environmental threats. The risk analysis also identifies the nature of each threat or vulnerability and how each may damage information security.

The Security Officer engages a qualified independent organization to conduct an accurate and thorough risk analysis that includes vulnerabilities, threats, likelihood, and impact, in accordance with all internal and external requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.5 - Identify Threats	Identify and document threats, both internal and external.	Fully Implemented

ID.RA-4 - Identify impacts

ID.RA-4: Potential business impacts and likelihoods are identified.

Overall Assessment: **Addressed**

Comments:

Detected events are analyzed to understand attack targets and methods. Event data is aggregated and correlated from multiple sources and sensors. Impact of events is determined.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.7 - Event Impact Determination	Ensure that the impact of events is determined.	Fully Implemented
CC19.7 - Understand Incident Impact	Ensure that the impact of an incident is understood.	Fully Implemented

ID.RA-5 - Determining risk

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

Overall Assessment: **Addressed**

Comments:

The organization has develop a comprehensive written plan to continue business during, or resume business immediately after, a disruption or disaster.

This plan goes beyond the tasks required to recover the organization’s IT infrastructure, and includes a Business Impact Analysis to identify the organization’s functions and the effect of critical functions

The Security Officer ensures that a Business Continuity Plan is created that identifies potential disruptions and disasters, defines mitigation strategies, and procedures to follow to ensure continued delivery of services and other critical functions.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC14.9 - Business Impact Analysis	Conduct Business Impact Anlyses (BIA) with all departments to measure the financial, regulatory, and reputational impact of incidents.	Fully Implemented
CC14.10 - Likelihood Analysis	Determine the likelihood of an incident based on historical information and other resources.	Fully Implemented
CC17.7 - Risk Determination	Determine risk using threats, vulnerabilities, likelihoods, and impacts.	Fully Implemented

ID.RA-6 - Risk responses

ID.RA-6: Risk responses are identified and prioritized

Overall Assessment: **Addressed**

Comments:

The Security Officer has implemented a comprehensive risk-management program based on the results of the risk analysis. Risk remediation, reduction, sharing, or acceptance plans will be based on the organization’s regulatory requirements or tolerance for risk.

The risk-management plan clearly describes the magnitude of the risks that are to be managed to a level acceptable to all stakeholders. Incident thresholds are identified to support the Incident Response Plan.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.8 - Risk Responses	Risk responses are identified and	Fully Implemented

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
	prioritized.	

ID.RM-1 - Risk management processes

ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.

Overall Assessment: **Addressed**

Comments:

The Security Officer has implemented a comprehensive risk-management program based on the results of the risk analysis. Risk remediation, reduction, sharing, or acceptance plans will be based on the organization’s regulatory requirements or tolerance for risk.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.9 - Risk Management	Establish and manage risk management processes as agreed to by organizational stakeholders.	Fully Implemented

ID.RM-2 - Organizational risk tolerance

ID.RM-2: Organizational risk tolerance is determined and clearly expressed.

Overall Assessment: **Addressed**

Comments:

The organization management has the right to determine its acceptable tolerance for risk. However, the organization will not accept risks that violate state, federal, or industry regulations such as data breach laws, HIPAA, or the Payment Card Industry Data Security Standard (PCI-DSS).

The Security Officer periodically meets with senior leadership and other stakeholders to review current risks and identify the organization’s tolerance for risk, considering all internal and external requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.10 - Risk Tolerance	Organization risk tolerance is determined and clearly expressed.	Fully Implemented

ID.RM-3 - Risk tolerance determination

ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

Overall Assessment: **Addressed**

Comments:

The organization management has, by right, determined its acceptable tolerance for risk. However, the organization will not accept risks that violate state, federal, or industry regulations such as data breach laws, HIPAA, or the Payment Card Industry Data Security Standard (PCI-DSS).

The Security Officer periodically meets with senior leadership and other stakeholders to review current risks and identify the organization’s tolerance for risk, considering all internal and external requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.11 - Risk Tolerance Alignment	Risk management aligns with all legal and regulatory requirements, the organization's role in critical infrastructure, and a sector-specific risk analysis.	Fully Implemented

PR.AC-1 - Identities and credentials

PR.AC-1: Identities and credentials are managedÂ for authorized devices and users.

Overall Assessment: **Addressed**

Comments:

The Security Officer has implemented procedures to ensure appropriate security of devices and users. Upon hiring or otherwise being authorized to access the organization’s IT assets, written authorization must be sent to the IT department and system administrators requesting access for the user. Changes must be requested in writing.

Users must acknowledge in writing their willingness to comply with the organization’s policies and procedures.

The IT department and system administrators will provision the minimum level of access required.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC7.1 - Identity Management	Manage identities and credentials for authorized devices and users.	Fully Implemented

PR.AC-2 - Physical access

PR.AC-2: Physical access to assets is managed and protected.

Overall Assessment: **Addressed**

Comments:

The Security Officer ensures that physical access to all internal and external assets that can connect to the organization’s IT resources is controlled to ensure consistent security and compliance.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC7.2 - Physical Access Management	Manage and protect physical access to assets.	Fully Implemented

PR.AC-3 - Remote access

PR.AC-3: Remote access is managed.

Overall Assessment: **Addressed**

Comments:

The Security Officer determines the appropriate tools and processes required to protect company data from loss, theft, and unauthorized access. This includes remote access mechanisms, security tools, methods of authentication, access logging, information system activity reviews, physical security of remote devices, virtual environments, and cloud-based solutions.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC7.3 - Remote Access Management	Manage remote access to assets.	Fully Implemented

PR.AC-4 - Access permissions

PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

Overall Assessment: **Addressed**

Comments:

The Security Officer has implemented processes and tools to ensure that users are provided with the minimum level of access required to do their jobs. For example, users will only be given access to network shares and database sections with the information required for their jobs. Network shares are reviewed to ensure that sensitive, confidential, or regulated data is not mistakenly saved in locations accessible by unauthorized users. For situations where access cannot be limited, tools must be utilized to log activity. User activity is periodically reviewed to identify any access beyond the minimum required. Unauthorized activity will result in discipline.

Wherever possible, duties of security personnel and management are separated to protect the organization against a rogue employee or accidental violation of security requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC7.4 - Access Permission Management	Manage access permissions, incorporating the principles of least privilege and separation of duties.	Fully Implemented

PR.AC-5 - Network integrity

PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.

Overall Assessment: **Not Addressed**

Comments:

No comments.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC7.5 - Network Segregation	Protect network integrity, incorporating network segregation where appropriate.	Planned

PR.AT-1 - Training

PR.AT-1: All users are informed and trained.

Overall Assessment: **Not Addressed**

Comments:

Yes - Partially Addressed

The Security Officer has implemented a security awareness and training program for all members of the organization’s workforce, including professional staff, company partners, and management.

The training program covers:
- The definition of security (availability, integrity, confidentiality)
- Threats to security (natural, human, and environmental)
- Methods of safeguarding security
- Security features of the organization's information system and applications
- Use of major applications
- Policies on installation and configuration of software
- Controls on access to information
- Correct use of anti-malware software
- Contingency plans and disaster procedures
- Workstation policies
- Good security practices (workstation use policies)
- Security incident reporting procedures
- User ID and password policies

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC16.1 - Workforce Training	Implement workforce training that covers all required policies and procedures.	Partially Implemented

PR.AT-2 - Privileged users

PR.AT-2: Privileged users understand roles & responsibilities.

Overall Assessment: **Addressed**

Comments:

The Security Officer is responsible for developing and implementing a security awareness and training program for all members of the organization’s workforce, including professional staff, company partners, and management.

The training program covers:
- Privileged user access to organizational systems and their roles and responsibilities.

New workforce members receive security training as part of their orientation.

The Security Officer has developed a training program that meets the organization’s needs, and work with HR and other stakeholders to ensure that all workforce members and applicable third parties receive initial and ongoing training. To ensure continued vigilance, training must be supplemented with an awareness program that includes reminders during meetings, plus signage, e-mails, and other communications.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.12 - Privileged Users	Ensure privileged users understand roles & responsibilities	Fully Implemented

PR.AT-3 - Third-party stakeholders

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

Overall Assessment: **Addressed**

Comments:

The Security Officer is responsible for developing and implementing a security awareness and training program for all members of the organization’s workforce, including professional staff, company partners, and management.

The training program covers:
• Third-party stakeholders, including contractors and consultants, will receive training and/or information on the organization's security policies and procedures.

The Security Officer has developed a training program that meets the organization’s needs, and work with HR and other stakeholders to ensure that all workforce members and applicable third parties receive initial and ongoing training. To ensure continued vigilance, training must be supplemented with an awareness program that includes reminders during meetings, plus signage, e-mails, and other communications.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.13 - Third-Parties	Ensure third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Fully Implemented

PR.AT-4 - Senior executives

PR.AT-4: Senior executives understand roles & responsibilities.

Overall Assessment: **Addressed**

Comments:

The Security Officer is responsible for developing and implementing a security awareness and training program for all members of the organization’s workforce, including professional staff, company partners, and management.

The training program covers:
• Senior executives will receive training and/or information on the organization's security policies and procedures.

The Security Officer has developed a training program that meets the organization’s needs, and work with HR and other stakeholders to ensure that all workforce members and applicable third parties receive initial and ongoing training. To ensure continued vigilance, training must be supplemented with an awareness program that includes reminders during meetings, plus signage, e-mails, and other communications.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.14 - Senior Executives	Ensure senior executives understand roles & responsibilities.	Fully Implemented

PR.AT-5 - Physical and information security personnel

PR.AT-5: Physical and information security personnel understand roles & responsibilities.

Overall Assessment: **Addressed**

Comments:

The Security Officer has developed a training program that meets the organization’s needs, and work with HR and other stakeholders to ensure that all workforce members and applicable third parties receive initial and ongoing training. To ensure continued vigilance, training must be supplemented with an awareness program that includes reminders during meetings, plus signage, e-mails, and other communications.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC2.15 - Physical Security Personnel	Ensure physical security personnel understand their roles & responsibilities and are trained to perform them.	Fully Implemented

PR.DS-1 - Data-at-rest

PR.DS-1: Data-at-rest is protected

Overall Assessment: **Addressed**

Comments:

When provisioned by the IT department and system administrators, all users will be set up with Unique User Identification. Periodic audits of access logs is conducted, and access is verified with randomly selected or targeted users. Third parties are also reviewed to ensure that individual users can be identified.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.1 - Protect Data	Ensure data-at-rest (stored) is protected.	Fully Implemented

PR.DS-2 - Data-in-transit

PR.DS-2: Data-in-transit is protected.

Overall Assessment: **Addressed**

Comments:

The Security Officer determines the appropriate tools and processes required to protect company data from loss, theft, and unauthorized access while data is in transit. This includes remote access mechanisms, security tools, methods of authentication, access logging, information system activity reviews, physical security of remote devices, virtual environments, and cloud-based solutions.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC13.1 - In-transit Data Protection	Ensure data-in-transit is protected.	Fully Implemented

PR.DS-3 - Asset management

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.

Overall Assessment: **Not Addressed**

Comments:

The Security Officer plans to implement controls and audit practices to prevent the removal of data, including controls to prevent e-mailing or storing data on removable media.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.2 - Manage Assets	Ensure assets are formally managed throughout removal, transfers, and disposition.	Not Implemented

PR.DS-4 - Capacity

PR.DS-4: Adequate capacity to ensure availability is maintained

Overall Assessment: **Not Addressed**

Comments:

The Security Officer plans to identify and oversee the implementation of systems and processes to ensure that availability is maintained by ensuring adequate capacity according to the organization’s policies.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.3 - Ensure Adequate Capacity	Ensure there is adequate capacity to ensure availability is maintained.	Not Implemented

PR.DS-5 - Data leak protection

PR.DS-5: Protections against data leaks are implemented

Overall Assessment: **Not Addressed**

Comments:

The Security Officer plans to implement systems and processes to ensure that data leaks are prevented according to the organization’s policies.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.4 - Protect Against Data Leaks	Protections against data leaks are implemented.	Not Implemented

PR.DS-6 - Integrity checking

PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity

Overall Assessment: **Addressed**

Comments:

The Security Officer has implemented systems and processes to ensure that software, firmware, and information integrity is maintained according to the organization’s policies.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.5 - Integrity Checking	Use integrity checking mechanisms to verify software, firmware, and information integrity.	Fully Implemented

PR.DS-7 - Development & testing environments

PR.DS-7: The development and testing environment(s) are separate from the production environment

Overall Assessment: **Not Addressed**

Comments:

The Security Officer is in the process of assessing the requirements that must be met to create a separate development and testing environment(s) according to the organization’s policies.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.6 - Separate Development & Testing Environments	Separate development and testing environment(s) from the production environment.	Not Implemented

PR.IP-1 - Baseline configurations

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.

Overall Assessment: **Addressed**

Comments:

The Security Officer develops and communicates baseline configurations and a written System Development Life Cycle to ensure that all devices and services provide an adequate level of security to meet the needs of the organization. The life cycle takes into consideration performance, security, and the needs of the organization to remain competitive in its markets.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC1.5 - Baseline Configurations	Establish and maintain baseline configurations of organizational systems (including hardware, portable media, mobile	Fully Implemented

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
	devices, industrial control systems, physical security systems, software, cloud services, firmware, and reporting requirements) throughout the respective system development life cycles.	

PR.IP-2 - System Development Life Cycle

PR.IP-2: A System Development Life Cycle to manage systems is implemented

Overall Assessment: **Addressed**

Comments:

The Security Officer has developed and communicated to the organization the baseline configurations and a written System Development Life Cycle to ensure that all devices and services provide an adequate level of security to meet the needs of the organization. This life cycle should consider performance, security, and the needs of the organization to remain competitive in its markets.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.7 - Implement Life Cycle	Implement a System Development Life Cycle to manage systems.	Fully Implemented

PR.IP-3 - Configuration change control

PR.IP-3: Configuration change control processes are in place.

Overall Assessment: **Addressed**

Comments:

The organization:
• Determines the types of changes to the information system that are configuration controlled;
• Approves configuration-controlled changes to the system with consideration for security;
• Documents approved configuration-controlled changes to the system;
• Retains and reviews records of configuration-controlled changes to the system;
• Audits activities associated with configuration-controlled changes to the system; and
• Coordinates and provides oversight for configuration change control activities through change request forms that must be approved by the Security Officer.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.8 - Change Controls	Ensure configuration change control processes are in place.	Fully Implemented

PR.IP-4 - Backups

PR.IP-4: Backups of information are conducted, maintained, and tested periodically

Overall Assessment: **Not Addressed**

Comments:

Yes - Partially

The Security Officer has implemented systems and processes to ensure that all data is backed up.

During a recent review of these processes it was identified that the backups related to Cloud Services provided by third parties did not meet the requirements necessary restore critical functions after an incident.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC14.13 - Backups	Ensure all business-critical and regulated data is backed up regularly to meet the organization's recovery priorities. Include local devices, hosted environments, and software-as-a-service platforms. Backups must be complete and comprehensive enough to restore critical functions.	Partially Implemented
CC14.15 - Restoration Testing	Ensure that backups are fully tested on a regular schedule to ensure that recoveries can take place as planned.	Partially Implemented

PR.IP-5 - Physical operating environment

PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.

Overall Assessment: **Addressed**

Comments:

The Security Officer develops and implements policies and procedures that allow only authorized workforce members and contractors to physically access the organization’s electronic information systems. The areas of the company's facilities in which components of its information systems are housed are physically secure and deny access to all but properly authorized workforce members.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC11.1 - Physical Access Policies	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Fully Implemented

PR.IP-6 - Data destruction

PR.IP-6: Data is destroyed according to policy.

Overall Assessment: **Not Addressed**

Comments:

No comments.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.10 - Data Destruction	Ensure data is destroyed according to policy, including deleting data no longer required for business purposes, and beyond any regulated retention period.	Not Implemented

PR.IP-7 - Continuous improvement

PR.IP-7: Protection processes are continuously improved.

Overall Assessment: **Not Addressed**

Comments:

Yes - Partially

The Security Officer conducts process reviews with key stakeholders at least annually to ensure that security is maintained according to the organization’s policies. Additional investments are planned to enable the identification of new threats and detection of access to data that does not comply with regulatory requirements that apply to the organization.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.13 - Improve Processes	Continuously improve data protection processes.	Partially Implemented

PR.IP-8 - Sharing information

PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties.

Overall Assessment: **Addressed**

Comments:

The Security Officer conducts process reviews with key stakeholders at least annually to ensure that security is maintained according to the organization’s policies.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.14 - Share Effectiveness Information	Share the effectiveness of protection technologies with appropriate parties.	Fully Implemented

PR.IP-9 - Incident Response and Business Continuity Plans

PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.

Overall Assessment: **Not Addressed**

Comments:

The Security Officer ensures that a Business Continuity Plan has been implemented that identifies potential disruptions and disasters, defines mitigation strategies, and procedures to follow to ensure continued delivery of services and other critical functions. Business Continuity Plan has been reviewed to ensure that all regulatory requirements have been met.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.41 - Incident Management Process	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Fully Implemented
CC14.1 - Business Continuity & Disaster Recovery Plans	Write effective Business Continuity and Disaster Recovery plans that meet all regulatory requirements and are in place and managed.	Partially Implemented

PR.IP-10 - Incident response and recovery plan testing

PR.IP-10: Response and recovery plans are tested.

Overall Assessment: **Not Addressed**

Comments:

The Security Officer has implemented systems and processes to ensure that all data is backed up.

This includes:

• Ensuring that all locations where data is stored are backed up
• Preventing data from being stored in locations that are not backed up
• Validating that backups are successful by testing them instead of relying on messages
• Multiple versions of backups are retained to enable access to at least 3 versions in case a document becomes corrupt
• Data is backed up to geographically-diverse locations highly unlikely to be affected by the same disruption or disaster
• Backup systems are compliant with all applicable regulations
• Unauthorized users are prevented from accessing the organization's data in a backup environment
• Backup plans are documented to comply with all applicable requirements

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC14.12 - Data Backup Plan	Write a comprehensive data backup plan that identifies the locations of all business-critical and regulated data, and the detailed process used to create and test backups.	Fully Implemented
CC14.18 - Recovery Capability Testing	Ensure that restoration testing proves that the RTO and RPO's can be met. If not, adjust the RTO and RPO to what has been proven to be possible, or change the proceses to meet the desired RTO and RPO.	Not Implemented

PR.IP-11 - Human Resource practices

PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

Overall Assessment: **Not Addressed**

Comments:

Yes - Partially

The Security Officer and HR Director plans to oversee a new implementation of processes to ensure that security is maintained according to the organization’s policies.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC7.6 - HR Cybersecurity Alignment	Ensure that cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	Partially Implemented

PR.IP-12 - Vulnerability management

PR.IP-12: A vulnerability management plan is developed and implemented

Overall Assessment: **Addressed**

Comments:

At-risk software or devices is immediately be removed or isolated to ensure that data is fully protected and that the organization maintains compliance with regulations and other requirements

Encryption status assessments are not performed by the organization at this time.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.2 - Vulnerability Plan	Ensure that a written vulnerability management plan is developed and implemented.	Fully Implemented

PR.MA-1 - Maintenance

PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

Overall Assessment: **Addressed**

Comments:

The Security Officer oversees appropriate maintenance support, including contractual service level agreements, to ensure that security is maintained according to the organization’s policies.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC9.2 - Perform & Control	Ensure maintenance and repair of	Fully Implemented

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
Maintenance & Repairs	organizational assets is performed and logged in a timely manner, with approved and controlled tools.	

PR.MA-2 - Remote maintenance

PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

Overall Assessment: **Addressed**

Comments:

The Security Officer oversees the implementation of security tools and processes to ensure that remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC9.4 - Manage Remote Maintenance	Ensure that remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	Fully Implemented

PR.PT-1 - Logging & Audit Controls

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Overall Assessment: **Addressed**

Comments:

The organization enables logging on all systems that offer the feature, including domain controllers, firewalls, and application programs. Logs are maintained for six years.
- Logs are reviewed at least each calendar quarter by the Security Officer or his/her designee.
- Log reviews are documented by a work ticket which will be maintained for six years.
- Logs are to provided to investigators, including law enforcement, to assist with incident response.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC10.1 - Implement Logging/Audit Controls	Ensure that audit/log records are implemented to record and examine activities on local devices, network devices,	Fully Implemented

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
	and cloud services.	

PR.PT-2 - Removable media

PR.PT-2: Removable media is protected and its use restricted according to policy.

Overall Assessment: **Addressed**

Comments:

The Security Officer has implemented security tools and processes to ensure the security of removable media.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.15 - Protect & Restrict Removable Media	Ensure that removable media is protected and its use restricted according to policy.	Fully Implemented

PR.PT-3 - Least functionality

PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.

Overall Assessment: **Addressed**

Comments:

The Security Officer and system administrators oversee the implementation of security tools and processes to ensure the concept of least functionality.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC8.16 - Control & Limit Access	Ensure that access to systems and assets is controlled, incorporating the principle of least functionality.	Fully Implemented

PR.PT-4 - Communications protection

PR.PT-4: Communications and control networks are protected

Overall Assessment: **Addressed**

Comments:

The organization controls, monitors, manages and protects communications and transmissions between information systems.

The Security Officer has established the requirements for protections such as link encryption, secure file transmission protocols, retention of files on source and destination systems, integrity validation, and restrictions for access at all levels (i.e. user/process, system, and network).

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC13.5 - Monitor, Control, and Protect Communications	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Fully Implemented

RC.CO-1 - Manage public relations

RC.CO-1: Public relations are managed.

Overall Assessment: **Addressed**

Comments:

For all incidents, public relations is managed based on the advice of legal counsel and insurance providers to ensure that the organization’s reputation is repaired.

Recovery activities are communicated to internal stakeholders and executive and management teams.

The organization identifies internal and external resources to protect its reputation and communicate recovery activities.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC20.4 - Manage Public Relations	Ensure public relations are managed.	Fully Implemented

RC.CO-2 - Reputation repair

RC.CO-2: Reputation after an event is repaired

Overall Assessment: **Addressed**

Comments:

For all incidents, public relations is managed based on the advice of legal counsel and insurance providers to ensure that the organization’s reputation is repaired.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC20.5 - Reputation Repair	Ensure that the organization's reputation after an event is repaired.	Fully Implemented

RC.CO-3 - Communicate recovery activities

RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

Overall Assessment: **Addressed**

Comments:

In response to an incident, recovery activities are communicated to internal stakeholders and executive and management teams.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC20.6 - Communicate Recovery Activities	Ensure that recovery activities are communicated to internal stakeholders and executive and management teams.	Fully Implemented

RC.IM-1 - Recovery lessons learned

RC.IM-1: Recovery plans incorporate lessons learned.

Overall Assessment: **Addressed**

Comments:

The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC20.2 - Recovery Plan Lessons Learned	Ensure recovery plans incorporate lessons learned.	Fully Implemented

RC.IM-2 - Update recovery strategies

RC.IM-2: Recovery strategies are updated.

Overall Assessment: **Addressed**

Comments:

The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC20.3 - Update Recovery Strategies	Ensure recovery strategies are updated.	Fully Implemented

RC.RP-1 - Execute recovery plan

RC.RP-1: Recovery plan is executed during or after an event

Overall Assessment: **Addressed**

Comments:

Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. As a part of the incident response review process, it is verified that any required recovery plans have been executed.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC20.1 - Follow Incident Recovery Plan	Ensure the recovery plan is executed during or after an event.	Fully Implemented

RS.AN-1 - Investigate notifications

RS.AN-1: Notifications from detection systems are investigated.Â

Overall Assessment: **Addressed**

Comments:

The Security Officer investigates security incidents and determine:
1. Whether a breach of security has occurred

2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused
3. Impact on critical business systems and processes along with organizational regulatory compliance requirements.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.8 - Investigate Detection System Notifications	Ensure that notifications from detection systems are investigated.	Fully Implemented

RS.AN-2 - Incident impact

RS.AN-2: The impact of the incident is understood.

Overall Assessment: **Addressed**

Comments:

Detected events are analyzed to understand attack targets and methods. Event data is aggregated and correlated from multiple sources and sensors. Impact of events is determined.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC18.7 - Event Impact Determination	Ensure that the impact of events is determined.	Fully Implemented

RS.AN-3 - Perform forensics

RS.AN-3: Forensics are performed.

Overall Assessment: **Addressed**

Comments:

The Security Officer must investigate security incidents and determine:
1. Whether a breach of security has occurred
2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused
3. Incident forensics are performed by certified forensic experts.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.5 - Perform Forensics	Ensure that forensics are performed.	Fully Implemented

RS.AN-4 - Categorize incidents

RS.AN-4: Incidents are categorized consistent with response plans.

Overall Assessment: **Not Addressed**

Comments:

The organization intends to implement a process to categorize incidents based on the guidance provided in the NIST SP 800-53 requirement outlined below:

CP-2: Contingency Plan

IR-4: Incident Handling

IR-5: Incident Monitoring

IR-8: Incident Response Plan

RA-3: Risk Assessment

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.6 - Categorize Incidents	Ensure that incidents are categorized consistent with response plans.	Not Implemented

RS.CO-1 - Response roles and responsibilities.

RS.CO-1: Personnel know their roles and order of operations when a response is needed.

Overall Assessment: **Addressed**

Comments:

The Security Officer has implemented processes, training, and accountability report to ensure that personnel know their roles and order of operations when a response is needed.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.14 - Personnel Incident Responsibilities	Ensure that personnel know their roles, limitations, and order of operations when a response is needed.	Fully Implemented

RS.CO-2 - Event reporting

RS.CO-2: Events are reported consistent with established criteria.

Overall Assessment: **Not Addressed**

Comments:

No comments.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.15 - Incident Reporting Determination	Determine that the incident meets the requiremends for reporting.	Not Implemented
CC19.16 - Incident Documentation & Reporting	Ensure that events are documented and reported consistent with established criteria, including all legal and regulatory requirements.	Partially Implemented

RS.CO-3 - Response information sharing

RS.CO-3: Information is shared consistent with response plans.

Overall Assessment: **Addressed**

Comments:

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.17 - Incident Information Sharing	Ensure that information is shared consistent with response plans.	Fully Implemented

RS.CO-4 - Response coordination

RS.CO-4: Coordination with stakeholders occurs consistent with response plans

Overall Assessment: **Addressed**

Comments:

Events are confidentially reported to management and key stakeholders, including legal counsel and insurance provider. Based on advice of legal counsel and insurance provider, information should be with external stakeholders to achieve broader cybersecurity situational awareness.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.19 - Stakeholder Incident Coordination	Ensure that coordination with stakeholders occurs consistent with response plans, legal advice, law enforcement requirements, and direction from the insurance company.	Fully Implemented

RS.CO-5 - Voluntary information sharing

RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

Overall Assessment: **Not Addressed**

Comments:

No comments.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.20 - Stakeholder Information Sharing	Ensure that voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness, consistent with response plans, legal advice, law enforcement requirements, and direction from the insurance company.	Not Implemented

RS.IM-1 - Response lessons learned

RS.IM-1: Response plans incorporate lessons learned.

Overall Assessment: **Not Addressed**

Comments:

Yes - Partially

The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.21 - Response Plan Lessons Learned		Implemented with Issues

RS.IM-2 - Update response strategies

RS.IM-2: Response strategies are updated

Overall Assessment: **Addressed**

Comments:

The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.22 - Update Response Strategies	Ensure response strategies are updated.	Fully Implemented

RS.MI-1 - Contain incidents

RS.MI-1: Incidents are contained

Overall Assessment: **Addressed**

Comments:

The Security Officer investigates security incidents and determine:
1. Whether a breach of security has occurred
2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused
3. Contain incidents to minimize organizational impact

The Security Officer ensures that actions needed to repair any damage caused or potentially caused by a security incident are taken.

The Security Officer documents the report of a security incident, the findings of the investigation, and any actions taken in response to those findings.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.3 - Contain Incidents	Ensure that incidents are contained.	Fully Implemented

RS.MI-2 - Mitigate incidents

RS.MI-2: Incidents are mitigated

Overall Assessment: **Addressed**

Comments:

Incidents are contained and mitigated. Newly identified vulnerabilities are mitigated or documented as accepted risks by the Security Officer.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.4 - Mitigate Incidents	Ensure that incidents are mitigated.	Fully Implemented

RS.MI-3 - Newly identified vulnerabilities

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.

Overall Assessment: **Addressed**

Comments:

Newly identified vulnerabilities are mitigated or documented as accepted risks by the Security Officer in accordance with the organization's security policy.

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC17.12 - Newly-Identified Vulnerabilities	Ensure that newly identified vulnerabilities are mitigated or documented as accepted risks.	Fully Implemented

RS.RP-1 - Execute response plans

RS.RP-1: Response plan is executed during or after an event.

Overall Assessment: **Addressed**

Comments:

The Security Officer oversees the implementation of Security Incident Response and Recovery Plans, conducts tests of critical processes at least annually, and conducts reviews with key stakeholders at least annually to ensure that security is maintained according to the organization’s policies

Internal Controls

CONTROL	DESCRIPTION	IMPLEMENTATION STATUS
CC19.1 - Incident Response Plan	Ensure that an effective Incident Response Plan is in place and managed.	Fully Implemented

4 - Internal Controls

CC1.1 - Inventories

Establish and maintain inventories of organizational systems (including hardware, hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, and firmware) throughout the respective system development life cycles.

Overall Assessment: **Fully Implemented**

Comments:

Hardware Inventory Procedure: The organization will utilize an automated tool to scan our network to identify assets at least each calendar quarter. Manual inventories will supplement the automated tools to document devices and systems that cannot be identified through automation. Software Inventory Procedure: The organization will utilize an automated tool to scan our network to identify software platforms and applications at least each calendar quarter. Manual inventories will supplement the automated tools to document platforms, applications, and cloud-based applications that cannot be identified through automation.

CC1.2 - Data Locations

Locate and identify all organizational data, including data stored on local devices, mobile devices, servers, mass storage, portable media, and cloud platforms.

Overall Assessment: **Fully Implemented**

Comments:

Access to data is to be controlled so that it may be accessed only by those with an approved need. Data must be stored in secure location on the network or in structured software environments. Data may not be removed from the organization's local network without specific authorization and may only be stored on secured devices. Data may only be accessed for authorized purposes. Snooping into the company's or workforce members' data or communications is expressly prohibited.

CC1.3 - Data Flow Mapping

Create a map of how data flows within and in/out of the organization.

Overall Assessment: **Fully Implemented**

Comments:

The organization has a data flow mapping process and associated exhibits from the last review of the data flows within the organization. The exhibits are updated when signification changes are made to information system components, user access rights, or the implementation of new business processes dependent on new or revised data flow processes.

CC1.5 - Baseline Configurations

Establish and maintain baseline configurations of organizational systems (including hardware, portable media, mobile devices, industrial control systems, physical security systems, software, cloud services, firmware, and reporting requirements) throughout the respective system development life cycles.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer develops and communicates baseline configurations and a written System Development Life Cycle to ensure that all devices and services provide an adequate level of security to meet the needs of the organization. The life cycle takes into consideration performance, security, and the needs of the organization to remain competitive in its markets.

CC2.1 - Organization's Supply Chain Role

Identify and communicate the organization's role in the supply chain.

Overall Assessment: **Fully Implemented**

Comments:

The organization's role in the supply chain is identified and communicated. This includes the organization's position with clients, vendors, and partners. The organization's place in critical infrastructure and its industry sector must be identified, documented, and communicated. Priorities for the organization's mission, objectives, and activities must be established, documented, and communicated. The Security Officer collaborates with internal and external stakeholders to ensure that critical services are identified and prioritized, and that adequate resources are dedicated to ensuring the delivery of services and resilience to disruptions and disasters.

CC2.2 - Organization's Critical Infrastructure Role

Identify and communicate the organization's role in critical infrastructure.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer collaborates with internal and external stakeholders to ensure that critical services are identified and prioritized, and that adequate resources are dedicated to ensuring the delivery of services and resilience to disruptions and disasters.

CC2.4 - Workforce Cybersecurity Roles & Responsibilities

Establish and document cybersecurity roles and responsibilities within the workforce.

Overall Assessment: **Fully Implemented**

Comments:

Only workforce members authorized by the organization's management may access client systems, and only for authorized purposes. Authorized workforce members must only use access control system approved by the organization to access client sites and data. Access is limited to the minimum required for the workforce members' role. Information and Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established. The organization's workforce members are required to maintain confidentiality of client information as if it was the organization's information. Specifically, Workforce members will only access client sites and data using approved mechanisms. No protected information may be removed from client site by physical or electronic means without specific authorization by the organization's management. If removal is approved, client data must be encrypted before transmission or physical movement No information overheard or seen at customer sites may be shared for purposes other than those authorized by the organization Workforce members will be trained on all regulations appropriate to their work with clients Workforce members will be subject to all civil and criminal penalties for non-compliance with regulations required of clients Any client information protected by federal, state, or industry regulations must be managed in accordance with those regulations. The Security Officer will classifies each type of workforce and third-party user's role and responsibilities and define appropriate access levels and capabilities.

CC2.8 - Roles & Responsibilities Coordination

Coordinate and align information security roles & responsibilities with internal roles and external partners.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer will classifies each type of workforce and third-party user's role and responsibilities and define appropriate access levels and capabilities.

CC2.11 - Detection Roles & Responsibilities

Ensure that roles and responsibilities for detection are well defined to ensure accountability.

Overall Assessment: **Fully Implemented**

Comments:

Roles and responsibilities for detection are well defined by the Security Officer to ensure accountability. Detection activities must comply with all applicable requirements. Processes must be tested and continuously improved. A baseline of network operations and expected data flows for users and systems must be established and managed. Detected events are analyzed to understand attack targets and methods. Event data are aggregated and correlated from multiple sources and sensors. Impact of events must be determined. Incident alert thresholds ae established by the Security Officer, who will review logs, either manually or through an automated process. IDS/IPS are especially helpful in identifying anomalies. Having network baselines helps rule out false positives in anomaly detection. Personnel activity is monitored to detect potential cybersecurity events. Suspected or proven event detection information is communicated to appropriate parties in time to comply with all applicable requirements. The Security Officer and system administrators oversee the implementation of security tools and processes to detect and manage unusual or unauthorized activity.

CC2.12 - Privileged Users

Ensure privileged users understand roles & responsibilities

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer is responsible for developing and implementing a security awareness and training program for all members of the organization's workforce, including professional staff, company partners, and management. The training program covers: Privileged user access to organizational systems and their roles and responsibilities. New workforce members receive security training as part of their orientation. The Security Officer has developed a training program that meets the organization's needs, and work with HR and other stakeholders to ensure that all workforce members and applicable third parties receive initial and ongoing training. To ensure continued vigilance, training must be supplemented with an awareness program that includes reminders during meetings, plus signage, e-mails, and other communications.

CC2.13 - Third-Parties

Ensure third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer is responsible for developing and implementing a security awareness and training program for all members of the organization's workforce, including professional staff, company partners, and management. The training program covers: Third-party stakeholders, including contractors and consultants, will receive training and/or information on the organization's security policies and procedures. The Security Officer has developed a training program that meets the organization's needs, and work with HR and other stakeholders to ensure that all workforce members and applicable third parties receive initial and ongoing training. To ensure continued vigilance, training must be supplemented with an awareness program that includes reminders during meetings, plus signage, e-mails, and other communications.

CC2.14 - Senior Executives

Ensure senior executives understand roles & responsibilities.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer is responsible for developing and implementing a security awareness and training program for all members of the organization's workforce, including professional staff, company partners, and management. The training program covers: Senior executives will receive training and/or information on the organization's security policies and procedures. The Security Officer has developed a training program that meets the organization's needs, and work with HR and other stakeholders to ensure that all workforce members and applicable third parties receive initial and ongoing training. To ensure continued vigilance, training must be supplemented with an awareness program that includes reminders during meetings, plus signage, e-mails, and other communications.

CC2.15 - Physical Security Personnel

Ensure physical security personnel understand their roles & responsibilities and are trained to perform them.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has developed a training program that meets the organization's needs, and work with HR and other stakeholders to ensure that all workforce members and applicable third parties receive initial and ongoing training. To ensure continued vigilance, training must be supplemented with an awareness program that includes reminders during meetings, plus signage, e-mails, and other communications.

CC3.1 - Legal and Regulatory Requirements

Identify and manage all legal and regulatory requirements.

Overall Assessment: **Fully Implemented**

Comments:

The organization uses commercially reasonable efforts to comply with all applicable laws and regulations, including: Federal and State Laws Industry Regulations Contracts Insurance Policy Requirements Information security roles & responsibilities will be coordinated and aligned with internal roles and external partners. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, must be understood and managed. Governance and risk management processes will address cybersecurity risks. The Security Officer has identified all relevant compliance requirements, classify each type of workforce and third-party user's role and responsibilities, and define appropriate access levels and capabilities. Processes will be developed to ensure compliance with all internal and external requirements.

CC4.1 - Written Cybersecurity Policies

Write policies addressing all cybersecurity requirements.

Overall Assessment: **Fully Implemented**

Comments:

The organization's security policy is reviewed by the organization's management each year and updated as necessary. The policy and any changes must be communicated to all workforce members. The Security Officer ensures that information security policies are established, reviewed, and updates as necessary.

CC5.1 - Risk Assessment/Risk Analysis

Periodically conduct an accurate and thorough assessment of the risks 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 data.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer periodically engages a qualified independent organization to conduct an accurate and thorough risk analysis that includes vulnerabilities, threats, likelihood, and impact, in accordance with all internal and external requirements.

CC5.2 - Prioritize Risks

Prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.

Overall Assessment: **Fully Implemented**

Comments:

The organization conducts periodic risk analysis to evaluate the likelihood and the impact that each security threat or vulnerability might occur. The risk analysis describes the nature and extent of the damage each threat might cause to the integrity, availability, and confidentiality of the organization's information resources. The risk analysis identifies high-priority threats that are the focus of risk-management efforts. Medium and low priority threats are also identified and reviewed for mitigation.

CC7.1 - Identity Management

Manage identities and credentials for authorized devices and users.

Overall Assessment: **Fully Implemented**

Comments:

Document the Password Management Plan here, or see the Organization Name - Password Management Plan.pdf attached to this Control Response using the "Upload Local File" feature below.

CC7.2 - Physical Access Management

Manage and protect physical access to assets.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer ensures that physical access to all internal and external assets that can connect to the organization's IT resources is controlled to ensure consistent security and compliance.

CC7.3 - Remote Access Management

Manage remote access to assets.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer determines the appropriate tools and processes required to protect company data from loss, theft, and unauthorized access. This includes remote access mechanisms, security tools, methods of authentication, access logging, information system activity reviews, physical security of remote devices, virtual environments, and cloud-based solutions.

CC7.4 - Access Permission Management

Manage access permissions, incorporating the principles of least privilege and separation of duties.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has implemented processes and tools to ensure that users are provided with the minimum level of access required to do their jobs. For example, users will only be given access to network shares and database sections with the information required for their jobs. Network shares are reviewed to ensure that sensitive, confidential, or regulated data is not mistakenly saved in locations accessible by unauthorized users. For situations where access cannot be limited, tools must be utilized to log activity. User activity is periodically reviewed to identify any access beyond the minimum required. Unauthorized activity will result in discipline. Wherever possible, duties of security personnel and management are separated to protect the organization against a rogue employee or accidental violation of security requirements.

CC7.5 - Network Segregation

Protect network integrity, incorporating network segregation where appropriate.

Overall Assessment: **Planned**

Comments:

No comments.

Action Plan Milestones:

Test Milestones

Changes to Action Plan Milestones:

Test changes to milestones

The actions planned to meet this requirement noted in the Plan of Action and Milestones Report.

CC7.6 - HR Cybersecurity Alignment

Ensure that cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).

Overall Assessment: **Partially Implemented**

Comments:

The Security Officer and HR Director plans to oversee a new implementation of processes to ensure that security is maintained according to the organization's policies.

CC8.1 - Protect Data

Ensure data-at-rest (stored) is protected.

Overall Assessment: **Fully Implemented**

Comments:

When provisioned by the IT department and system administrators, all users will be set up with Unique User Identification. Periodic audits of access logs is conducted, and access is verified with randomly selected or targeted users. Third parties are also reviewed to ensure that individual users can be identified.

CC8.2 - Manage Assets

Ensure assets are formally managed throughout removal, transfers, and disposition.

Overall Assessment: **Not Implemented**

Comments:

The Security Officer plans to implement controls and audit practices to prevent the removal of data, including controls to prevent e-mailing or storing data on removable media.

CC8.3 - Ensure Adequate Capacity

Ensure there is adequate capacity to ensure availability is maintained.

Overall Assessment: **Not Implemented**

Comments:

The Security Officer plans to identify and oversee the implementation of systems and processes to ensure that availability is maintained by ensuring adequate capacity according to the organization's policies.

CC8.4 - Protect Against Data Leaks

Protections against data leaks are implemented.

Overall Assessment: **Not Implemented**

Comments:

The Security Officer plans to implement systems and processes to ensure that data leaks are prevented according to the organization's policies.

CC8.5 - Integrity Checking

Use integrity checking mechanisms to verify software, firmware, and information integrity.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has implemented systems and processes to ensure that software, firmware, and information integrity is maintained according to the organization's policies.

CC8.6 - Separate Development & Testing Environments

Separate development and testing environment(s) from the production environment.

Overall Assessment: **Not Implemented**

Comments:

The Security Officer is in the process of assessing the requirements that must be met to create a separate development and testing environment(s) according to the organization's policies.

CC8.7 - Implement Life Cycle

Implement a System Development Life Cycle to manage systems.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has developed and communicated to the organization the baseline configurations and a written System Development Life Cycle to ensure that all devices and services provide an adequate level of security to meet the needs of the organization. This life cycle should consider performance, security, and the needs of the organization to remain competitive in its markets.

CC8.8 - Change Controls

Ensure configuration change control processes are in place.

Overall Assessment: **Fully Implemented**

Comments:

The organization: Determines the types of changes to the information system that are configuration controlled; Approves configuration-controlled changes to the system with consideration for security; Documents approved configuration-controlled changes to the system; Retains and reviews records of configuration-controlled changes to the system; Audits activities associated with configuration-controlled changes to the system; and Coordinates and provides oversight for configuration change control activities through change request forms that must be approved by the Security Officer.

CC8.10 - Data Destruction

Ensure data is destroyed according to policy, including deleting data no longer required for business purposes, and beyond any regulated retention period.

Overall Assessment: **Not Implemented**

Comments:

No comments.

CC8.13 - Improve Processes

Continuously improve data protection processes.

Overall Assessment: **Partially Implemented**

Comments:

The Security Officer conducts process reviews with key stakeholders at least annually to ensure that security is maintained according to the organization's policies. Additional investments are planned to enable the identification of new threats and detection of access to data that does not comply with regulatory requirements that apply to the organization.

CC8.14 - Share Effectiveness Information

Share the effectiveness of protection technologies with appropriate parties.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer conducts process reviews with key stakeholders at least annually to ensure that security is maintained according to the organization's policies.

CC8.15 - Protect & Restrict Removable Media

Ensure that removable media is protected and its use restricted according to policy.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has implemented security tools and processes to ensure the security of removable media.

CC8.16 - Control & Limit Access

Ensure that access to systems and assets is controlled, incorporating the principle of least functionality.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer and system administrators oversee the implementation of security tools and processes to ensure the concept of least functionality.

CC8.41 - Incident Management Process

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

Overall Assessment: **Fully Implemented**

Comments:

Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. Response and recovery plans are tested. Personnel are trained to know their roles and order of operations when a response is needed. The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed. The Security Officer oversees the implementation of Security Incident Response and Recovery Plans, conducts tests of critical processes at least annually, and conducts reviews with key stakeholders at least annually to ensure that security is maintained according to the organization's policies.

CC9.2 - Perform & Control Maintenance & Repairs

Ensure maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer oversees appropriate maintenance support, including contractual service level agreements, to ensure that security is maintained according to the organization's policies.

CC9.4 - Manage Remote Maintenance

Ensure that remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer oversees the implementation of security tools and processes to ensure that remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

CC10.1 - Implement Logging/Audit Controls

Ensure that audit/log records are implemented to record and examine activities on local devices, network devices, and cloud services.

Overall Assessment: **Fully Implemented**

Comments:

The organization enables logging on all systems that offer the feature, including domain controllers, firewalls, and application programs. Logs are maintained for six years. Logs are reviewed at least each calendar quarter by the Security Officer or his/her designee. Log reviews are documented by a work ticket which will be maintained for six years. Logs are to provided to investigators, including law enforcement, to assist with incident response.

CC11.1 - Physical Access Policies

Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer develops and implements policies and procedures that allow only authorized workforce members and contractors to physically access the organization's electronic information systems. The areas of the company's facilities in which components of its information systems are housed are physically secure and deny access to all but properly authorized workforce members.

CC13.1 - In-transit Data Protection

Ensure data-in-transit is protected.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer determines the appropriate tools and processes required to protect company data from loss, theft, and unauthorized access while data is in transit. This includes remote access mechanisms, security tools, methods of authentication, access logging, information system activity reviews, physical security of remote devices, virtual environments, and cloud-based solutions.

CC13.5 - Monitor, Control, and Protect Communications

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

Overall Assessment: **Fully Implemented**

Comments:

The organization controls, monitors, manages and protects communications and transmissions between information systems. The Security Officer has established the requirements for protections such as link encryption, secure file transmission protocols, retention of files on source and destination systems, integrity validation, and restrictions for access at all levels (i.e. user/process, system, and network).

CC14.1 - Business Continuity & Disaster Recovery Plans

Write effective Business Continuity and Disaster Recovery plans that meet all regulatory requirements and are in place and managed.

Overall Assessment: **Partially Implemented**

Comments:

The Security Officer ensures that a Business Continuity Plan has been implemented that identifies potential disruptions and disasters, defines mitigation strategies, and procedures to follow to ensure continued delivery of services and other critical functions. Business Continuity Plan has been reviewed to ensure that all regulatory requirements have been met.

CC14.2 - Resource Criticality

Establish and communicate the criticality of all resources.

Overall Assessment: **Partially Implemented**

Comments:

The Security Officer has implemented manual and automated processes to classify and secure the organization's resources (e.g., hardware, devices, data, and software). To date, the criticality of workforce member access to organization systems has not been established.

CC14.4 - Organizational Priorities

Establish and communicate priorities based on the organization's mission, objectives, activities, legal requirements, and regulations.

Overall Assessment: **Fully Implemented**

Comments:

The organization's place in critical infrastructure and its industry sector has been identified, documented, and communicated to all stakeholders. On an ongoing basis, priorities for the organization's mission, objectives, and activities are established, documented, and communicated periodically to all affected stakeholders.

CC14.7 - Dependencies

Identify and document all dependencies for each critical function. Include technology, people, and facilities.

Overall Assessment: **Fully Implemented**

Comments:

The organization's role in the supply chain is identified and communicated. This includes the organization's position with clients, vendors, and partners. The organization's place in critical infrastructure and its industry sector must be identified, documented, and communicated. Priorities for the organization's mission, objectives, and activities must be established, documented, and communicated. The Security Officer collaborates with internal and external stakeholders to ensure that critical services are identified and prioritized, and verifies that adequate resources are dedicated to ensuring the delivery of services and resilience to disruptions and disasters

CC14.8 - Resliency Requirements

Establish resilience requirements to support the delivery of critical services.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer collaborates with internal and external stakeholders to ensure that critical services are identified and prioritized, and that adequate resources are dedicated to ensuring the delivery of services and resilience to disruptions and disasters

CC14.9 - Business Impact Analysis

Conduct Business Impact Anlyses (BIA) with all departments to measure the financial, regulatory, and reputational impact of incidents.

Overall Assessment: **Fully Implemented**

Comments:

The organization has develop a comprehensive written plan to continue business during, or resume business immediately after, a disruption or disaster. This plan goes beyond the tasks required to recover the organization's IT infrastructure, and includes a Business Impact Analysis to identify the organization's functions and the effect of critical functions The Security Officer ensures that a Business Continuity Plan is created that identifies potential disruptions and disasters, defines mitigation strategies, and procedures to follow to ensure continued delivery of services and other critical functions.

CC14.10 - Likelihood Analysis

Determine the likelihood of an incident based on historical information and other resources.

Overall Assessment: **Fully Implemented**

Comments:

The organization has develop a comprehensive written plan to continue business during, or resume business immediately after, a disruption or disaster. This plan goes beyond the tasks required to recover the organization's IT infrastructure, and includes a Likelihood Analysis based on historical information and other resources to identify the organization's functions and the effect of critical functions The Security Officer ensures that a Business Continuity Plan is created that identifies potential disruptions and disasters, defines mitigation strategies, and procedures to follow to ensure continued delivery of services and other critical functions.

CC14.12 - Data Backup Plan

Write a comprehensive data backup plan that identifies the locations of all business-critical and regulated data, and the detailed process used to create and test backups.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has implemented systems and processes to ensure that all data is backed up. This includes: Ensuring that all locations where data is stored are backed up Preventing data from being stored in locations that are not backed up Validating that backups are successful by testing them instead of relying on messages Multiple versions of backups are retained to enable access to at least 3 versions in case a document becomes corrupt Data is backed up to geographically-diverse locations highly unlikely to be affected by the same disruption or disaster Backup systems are compliant with all applicable regulations Unauthorized users are prevented from accessing the organization's data in a backup environment Backup plans are documented to comply with all applicable requirements

CC14.13 - Backups

Ensure all business-critical and regulated data is backed up regularly to meet the organization's recovery priorities. Include local devices, hosted environments, and software-as-a-service platforms. Backups must be complete and comprehensive enough to restore critical functions.

Overall Assessment: **Partially Implemented**

Comments:

The Security Officer has implemented systems and processes to ensure that all data is backed up. During a recent review of these processes it was identified that the backups related to Cloud Services provided by third parties did not meet the requirements necessary restore critical functions after an incident.

CC14.15 - Restoration Testing

Ensure that backups are fully tested on a regular schedule to ensure that recoveries can take place as planned.

Overall Assessment: **Partially Implemented**

Comments:

Back-up data sets are tested to verify that they contain exact copies of the information that they back up and that the back-up data can be successfully restored.

CC14.18 - Recovery Capability Testing

Ensure that restoration testing proves that the RTO and RPO's can be met. If not, adjust the RTO and RPO to what has been proven to be possible, or change the proceses to meet the desired RTO and RPO.

Overall Assessment: **Not Implemented**

Comments:

No comments.

CC16.1 - Workforce Training

Implement workforce training that covers all required policies and procedures.

Overall Assessment: **Partially Implemented**

Comments:

The Security Officer has implemented a security awareness and training program for all members of the organization's workforce, including professional staff, company partners, and management. The training program covers: The definition of security (availability, integrity, confidentiality) Threats to security (natural, human, and environmental) Methods of safeguarding security Security features of the organization's information system and applications Use of major applications Policies on installation and configuration of software Controls on access to information Correct use of anti-malware software Contingency plans and disaster procedures Workstation policies Good security practices (workstation use policies) Security incident reporting procedures User ID and password policies

CC17.1 - Vulnerability Scans

Scan for vulnerabilities and encryption status in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Overall Assessment: **Partially Implemented**

Comments:

At-risk software or devices is immediately be removed or isolated to ensure that data is fully protected and that the organization maintains compliance with regulations and other requirements Encryption status assessments are not performed by the organization at this time.

CC17.2 - Vulnerability Plan

Ensure that a written vulnerability management plan is developed and implemented.

Overall Assessment: **Fully Implemented**

Comments:

At-risk software or devices is immediately be removed or isolated to ensure that data is fully protected and that the organization maintains compliance with regulations and other requirements Encryption status assessments are not performed by the organization at this time.

CC17.5 - Identify Threats

Identify and document threats, both internal and external.

Overall Assessment: **Fully Implemented**

Comments:

The organization's risk analysis process identifies threats to the security of the organization's company data, including natural, human, and environmental threats. The risk analysis also identifies the nature of each threat or vulnerability and how each may damage information security. The Security Officer engages a qualified independent organization to conduct an accurate and thorough risk analysis that includes vulnerabilities, threats, likelihood, and impact, in accordance with all internal and external requirements.

CC17.6 - Threat and Vulnerability Information

Receive and respond to threat and vulnerability information from information sharing forums and sources and communicate to stakeholders.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has implemented the necessary processes to access and use threat and vulnerability information is received from information sharing forums and sources as part of the organization's risk analysis process.

CC17.7 - Risk Determination

Determine risk using threats, vulnerabilities, likelihoods, and impacts.

Overall Assessment: **Fully Implemented**

Comments:

The organization's risk analysis process, implemented by the Security Officer, evaluates the likelihood and the impact that each security threat or vulnerability might occur.

CC17.8 - Risk Responses

Risk responses are identified and prioritized.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has implemented a comprehensive risk-management program based on the results of the risk analysis. Risk remediation, reduction, sharing, or acceptance plans will be based on the organization's regulatory requirements or tolerance for risk. The risk-management plan clearly describes the magnitude of the risks that are to be managed to a level acceptable to all stakeholders. Incident thresholds are identified to support the Incident Response Plan.

CC17.9 - Risk Management

Establish and manage risk management processes as agreed to by organizational stakeholders.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has implemented a comprehensive risk-management program based on the results of the risk analysis. Risk remediation, reduction, sharing, or acceptance plans will be based on the organization's regulatory requirements or tolerance for risk.

CC17.10 - Risk Tolerance

Organization risk tolerance is determined and clearly expressed.

Overall Assessment: **Fully Implemented**

Comments:

The organization management has the right to determine its acceptable tolerance for risk. However, the organization will not accept risks that violate state, federal, or industry regulations such as data breach laws, HIPAA, or the Payment Card Industry Data Security Standard (PCI-DSS). The Security Officer periodically meets with senior leadership and other stakeholders to review current risks and identify the organization's tolerance for risk, considering all internal and external requirements.

CC17.11 - Risk Tolerance Alignment

Risk management aligns with all legal and regulatory requirements, the organization's role in critical infrastructure, and a sector-specific risk analysis.

Overall Assessment: **Fully Implemented**

Comments:

The organization management has, by right, determined its acceptable tolerance for risk. However, the organization will not accept risks that violate state, federal, or industry regulations such as data breach laws, HIPAA, or the Payment Card Industry Data Security Standard (PCI-DSS). The Security Officer periodically meets with senior leadership and other stakeholders to review current risks and identify the organization's tolerance for risk, considering all internal and external requirements.

CC17.12 - Newly-Identified Vulnerabilities

Ensure that newly identified vulnerabilities are mitigated or documented as accepted risks.

Overall Assessment: **Fully Implemented**

Comments:

Newly identified vulnerabilities are mitigated or documented as accepted risks by the Security Officer in accordance with the organization's security policy.

CC18.2 - Triage Events

Analyze and triage events to support event resolution and incident declaration.

Overall Assessment: **Fully Implemented**

Comments:

Response and recovery plans are executed during or after an event. Notifications from detection systems are investigated and documented. The impact of the incident is analyzed and understood. Forensics are performed and incident are categorized.

CC18.6 - Event Data Correlation

Ensure that event data are aggregated and correlated from multiple sources and sensors.

Overall Assessment: **Fully Implemented**

Comments:

Detected events are analyzed to understand attack targets and methods. Event data is aggregated and correlated from multiple sources and sensors. Impact of events is determined.

CC18.7 - Event Impact Determination

Ensure that the impact of events is determined.

Overall Assessment: **Fully Implemented**

Comments:

Detected events are analyzed to understand attack targets and methods. Event data is aggregated and correlated from multiple sources and sensors. Impact of events is determined.

CC18.8 - Incident Alert Thresholds

Ensure that incident alert thresholds are established.

Overall Assessment: **Fully Implemented**

Comments:

Incident alert thresholds have been established by the Security Officer, who will review logs, either manually or through an automated process. IDS/IPS are especially helpful in identifying anomalies. Having network baselines helps rule out false positives in anomaly detection.

CC18.10 - Physical Environment Monitoring

Overall Assessment: **Fully Implemented**

Comments:

The organization utilizes perimeter alarm systems, mechanical and/or electronic access systems, video surveillance, security guards, and temperature and water alarms. Alarms will be set to alert workforce members and/or law enforcement/security services.

CC18.11 - Personnel Activity Monitoring

Ensure that personnel activity is monitored to detect potential cybersecurity events.

Overall Assessment: **Fully Implemented**

Comments:

Roles and responsibilities for detection are defined by the Security Officer to ensure accountability. Detection activities must comply with all applicable requirements. Processes must be tested and continuously improved. As a part of this process, personnel activity must be monitored to detect potential cybersecurity events.

CC18.12 - Malicious Code Detection

Ensure that malicious code is detected.

Overall Assessment: **Partially Implemented**

Comments:

All systems (including servers) and mobile devices are protected against malicious software (malware.) This includes maintaining current patch and firmware levels, using endpoint protection software, protecting the network and mobile devices with a business-class firewall running an active intrusion prevention system. All system and security patches is installed within 2 business days of being released. This includes operating systems, application software, malware definitions, and firewall intrusion prevention updates. Critical devices such as firewalls, network switches and infrastructure hardware, computers and servers, storage devices, and other equipment must be checked every 90-days for firmware updates. Anti-malware software is installed on all endpoint devices and servers to protect the organization and its information from attack by malicious software such as computer viruses, worms, and Trojan horses. This software must be maintained with current subscriptions and regularly updated; must be turned on; and must be installed to prevent users from disabling or removing the software. Workforce members are instructed to not disable anti-virus software and must immediately take action to report virus infections and remove viruses from affected machines when the anti-virus software identifies an infection After a recent periodic review of the status of anti-virus software installed on Windows computer endpoints using automated scanning and reporting tools, 32% of all computer endpoints have the automatic update functionality of the anti-virus software installed on the identified endpoints set to disabled. This incident has been reported and corrective action is underway.

CC18.13 - Mobile Code Detection

Ensure that unauthorized mobile code is detected.

Overall Assessment: **Fully Implemented**

Comments:

Mobile devices are protected against malicious software (malware.)

CC18.14 - Monitor Service Provider Activity

Ensure that external service provider activity is monitored to detect potential cybersecurity events.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer and other company leaders have implemented security processes to protect against risks from external service providers. Refer to the organization's system security plan for more specific information.

CC18.15 - Monitoring

Ensure that monitoring the network for unauthorized personnel, connections, devices, and software is performed.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer regularly reviews records associated with the monitoring of system activity to identify any patterns of activity that suggest the organization's security policies and procedures have been breached, either by members of its workforce or by outside individuals or organizations. The Security Officer determines whether security has been violated and takes appropriate corrective action, including changes in security policies and procedures.

CC18.16 - Detection Compliance

Ensure that detection activities comply with all applicable requirements.

Overall Assessment: **Fully Implemented**

Comments:

Roles and responsibilities for detection are well defined by the Security Officer to ensure accountability. Detection activities must comply with all applicable requirements. Processes are tested and continuously improved. Periodic reviews are performed to ensure that detection activities complete with legal and regulatory requirements.

CC18.17 - Test Detection Processes

Ensure that detection processes are tested.

Overall Assessment: **Fully Implemented**

Comments:

Incident alert thresholds must be established by the Security Officer, who will review logs, either manually or through an automated process. As a part of this review process, detection processes are tested and verified as operational in compliance with the organization's information security and risk management plans.

CC18.18 - Detection Information Communications

Ensure that event detection information is communicated to appropriate parties.

Overall Assessment: **Fully Implemented**

Comments:

Suspected or proven event detection information is communicated to appropriate parties in time to comply with all applicable requirements.

CC18.19 - Improve Detection Processes

Ensure that detection processes are continuously improved.

Overall Assessment: **Fully Implemented**

Comments:

Roles and responsibilities for detection are defined by the Security Officer to ensure accountability. Detection activities comply with all applicable requirements. Processes are periodically tested and continuously improved.

CC19.1 - Incident Response Plan

Ensure that an effective Incident Response Plan is in place and managed.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer oversees the implementation of Security Incident Response and Recovery Plans, conducts tests of critical processes at least annually, and conducts reviews with key stakeholders at least annually to ensure that security is maintained according to the organization's policies

CC19.3 - Contain Incidents

Ensure that incidents are contained.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer investigates security incidents and determine: 1. Whether a breach of security has occurred 2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused 3. Contain incidents to minimize organizational impact The Security Officer ensures that actions needed to repair any damage caused or potentially caused by a security incident are taken. The Security Officer documents the report of a security incident, the findings of the investigation, and any actions taken in response to those findings.

CC19.4 - Mitigate Incidents

Ensure that incidents are mitigated.

Overall Assessment: **Fully Implemented**

Comments:

Incidents are contained and mitigated. Newly identified vulnerabilities are mitigated or documented as accepted risks by the Security Officer.

CC19.5 - Perform Forensics

Ensure that forensics are performed.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer must investigate security incidents and determine: 1. Whether a breach of security has occurred 2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused 3. Incident forensics are performed by certified forensic experts.

CC19.6 - Categorize Incidents

Ensure that incidents are categorized consistent with response plans.

Overall Assessment: **Not Implemented**

Comments:

The organization intends to implement a process to categorize incidents based on the guidance provided in the NIST SP 800-53 requirement outlined below: CP-2: Contingency Plan IR-4: Incident Handling IR-5: Incident Monitoring IR-8: Incident Response Plan RA-3: Risk Assessment

CC19.7 - Understand Incident Impact

Ensure that the impact of an incident is understood.

Overall Assessment: **Fully Implemented**

Comments:

Response and recovery plans are executed during or after an event. Notifications from detection systems are investigated and documented. The impact of the incident are understood. Forensics must be performed and the incident are categorized

CC19.8 - Investigate Detection System Notifications

Ensure that notifications from detection systems are investigated.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer investigates security incidents and determine: 1. Whether a breach of security has occurred 2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused 3. Impact on critical business systems and processes along with organizational regulatory compliance requirements.

CC19.14 - Personnel Incident Responsibilities

Ensure that personnel know their roles, limitations, and order of operations when a response is needed.

Overall Assessment: **Fully Implemented**

Comments:

The Security Officer has implemented processes, training, and accountability report to ensure that personnel know their roles and order of operations when a response is needed.

CC19.15 - Incident Reporting Determination

Determine that the incident meets the requiremends for reporting.

Overall Assessment: **Not Implemented**

Comments:

No comments.

CC19.16 - Incident Documentation & Reporting

Ensure that events are documented and reported consistent with established criteria, including all legal and regulatory requirements.

Overall Assessment: **Partially Implemented**

Comments:

Security incidents are reported promptly to the Security Officer. This includes the mere suspicion that an incident might have occurred. Incidents, including attempts to discover someone's password, should be reported by the workforce members responsible for the incident or workforce members who identify the incident.

CC19.17 - Incident Information Sharing

Ensure that information is shared consistent with response plans.

Overall Assessment: **Fully Implemented**

Comments:

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

CC19.19 - Stakeholder Incident Coordination

Ensure that coordination with stakeholders occurs consistent with response plans, legal advice, law enforcement requirements, and direction from the insurance company.

Overall Assessment: **Fully Implemented**

Comments:

Events are confidentially reported to management and key stakeholders, including legal counsel and insurance provider. Based on advice of legal counsel and insurance provider, information should be with external stakeholders to achieve broader cybersecurity situational awareness.

CC19.20 - Stakeholder Information Sharing

Ensure that voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness, consistent with response plans, legal advice, law enforcement requirements, and direction from the insurance company.

Overall Assessment: **Not Implemented**

Comments:

No comments.

CC19.21 - Response Plan Lessons Learned

Overall Assessment: **Implemented with Issues**

Comments:

The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed.

CC19.22 - Update Response Strategies

Ensure response strategies are updated.

Overall Assessment: **Fully Implemented**

Comments:

The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed.

CC20.1 - Follow Incident Recovery Plan

Ensure the recovery plan is executed during or after an event.

Overall Assessment: **Fully Implemented**

Comments:

Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. As a part of the incident response review process, it is verified that any required recovery plans have been executed.

CC20.2 - Recovery Plan Lessons Learned

Ensure recovery plans incorporate lessons learned.

Overall Assessment: **Fully Implemented**

Comments:

The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed.

CC20.3 - Update Recovery Strategies

Ensure recovery strategies are updated.

Overall Assessment: **Fully Implemented**

Comments:

The response and recovery plans incorporate lessons learned from incidents, and strategies updated as needed.

CC20.4 - Manage Public Relations

Ensure public relations are managed.

Overall Assessment: **Fully Implemented**

Comments:

For all incidents, public relations is managed based on the advice of legal counsel and insurance providers to ensure that the organization's reputation is repaired. Recovery activities are communicated to internal stakeholders and executive and management teams. The organization identifies internal and external resources to protect its reputation and communicate recovery activities.

CC20.5 - Reputation Repair

Ensure that the organization's reputation after an event is repaired.

Overall Assessment: **Fully Implemented**

Comments:

For all incidents, public relations is managed based on the advice of legal counsel and insurance providers to ensure that the organization's reputation is repaired.

CC20.6 - Communicate Recovery Activities

Ensure that recovery activities are communicated to internal stakeholders and executive and management teams.

Overall Assessment: **Fully Implemented**

Comments:

In response to an incident, recovery activities are communicated to internal stakeholders and executive and management teams.