| Prepared For: Fossa University

S2ORG
Powered by S2SCORE

NIST Cybersecurity Framework Report

| **Date:** March 11, 2021

Table of Contents

About S2SCORE

Fossa University overall S2SCORE (or risk rating) is **551.70.**

A S2SCORE of **551.70** translates to "**Poor**". In general, a S2SCORE in this range means that there are a limited number of controls and safeguards that have been implemented to protect organizational assets. Vulnerabilities, to include critical, still exist and are in the presence of applicable threats. A compromise of vulnerabilities is possible and would cause a serious impact to the organization to include financial loss, lack of compliance with regulatory or contractual requirements, and impact to the company brand and reputation.

The S2SCORE is calculated in a range from 300 to 850. The lower the score, the higher the risk. And vice versa. A S2SCORE of **660.00** or "**Good**" is acceptable to most organizations and should be the goal for Fossa University.

The S2Score ranges are as follows:

- **Very Poor** (300 - 499)
- **Poor** (500 - 599)
- **Fair** (600 - 659)
- **Good** (660 - 779)
- **Excellent** (780 - 850)

How to Use this Report

Use this report to identify risk areas where your organization's controls may be insufficient to meet NIST CSF requirements.

Fossa University should aim to achieve a score of 850 or better for all NIST CSF controls requirements for full compliance. For any control where Fossa University is not is full compliance, a Plan of Actions & Milestones (POA&M) should be created and monitored by executive management.

Fossa University NIST CSF Gap Assessment Overall Results

Below is a gap assessment for your organization based on your responses to the S2SCORE assessment for NIST Cybersecurity Framework (NIST CSF), the Framework for Improving Critical Infrastructure Cybersecurity publication (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

This report is provided for informational purposes only and does not guarantee compliance with federal, state, or local laws. The information provided may not be applicable or appropriate for all organization responsible for the protection of assets related to or in support of the Critical Infrastructure. This gap assessment is not intended to be an exhaustive or definitive source on safeguarding critical infrastructure cybersecurity risks. For more information about the NIST CSF, please visit the NIST Cybersecurity Framework website: (https://www.nist.gov/cyberframework).

The Framework Core consists of five concurrent and continuous Functions:

- IDENTIFY (ID)
- PROTECT (PR)
- DETECT (DE)
- RESPOND (RS)

- RECOVER (RC)

The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function.

NIST CSF Function S2SCORES

The S2Org assessment scores, where applicable, and when aggregated, produce Function scores as depicted in the following table.

IDENTIFY (ID)	PROTECT (PR)	DETECT (DE)	RESPOND (RS)	RECOVER (RC)
604 Fair	635 Fair	593 Poor	607 Fair	617 Fair

The goal for most organizations is to score 660 (Good) or higher in each function.

NIST CSF Function and Category Heatmap

IDENTIFY (ID)	PROTECT (PR)	DETECT (DE)	RESPOND (RS)	RECOVER (RC)
Fair	Fair	Poor	Fair	Fair
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

Fossa University NIST CSF Gap Assessment Section Summary

IDENTIFY Function

Asset Management	Business Environment	Governance
530	657	665
Risk Assessment	**Risk Management Strategy**	**Supply Chain Risk**
595	644	513

NIST CSF IDENTIFY Function includes the following Categories:

- **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
- **Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- **Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- **Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Asset Management (ID.AM)

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

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

Statement	Statement Name	Status
P1.4.1.1	An asset management (or similar) policy has been developed and is sufficient in scope.	True
P1.4.1.2	Physical devices and systems within the organization are all inventoried.	True
P1.4.1.4	Asset management is supported by documented procedures.	False
P1.4.1.5	All physical, software, and data assets are formally accounted for throughout the organization.	False
P1.4.1.6	Roles and responsibilities for developing and maintaining an inventory of information processing facilities and data assets are formally defined by management.	False
P1.4.1.7	The organization's inventory of information assets is centrally managed.	True
P1.4.1.8	Formal asset reconciliation processes are sufficient to account for lost, damaged, and stolen assets.	False
P1.4.1.9	The organization's asset management practices account for the entire asset life-cycle.	True
P1.5.1.3	Physical and logical access controls are integrated and adequately considered in policy.	True
P4.3.1.1	The organization regularly audits the ports that are open to the Internet.	False

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

Statement	Statement Name	Status
P1.4.1.1	An asset management (or similar) policy has been developed and is sufficient in scope.	True
P1.4.1.3	Software platforms and applications within the organization are inventoried.	False
P1.4.1.4	Asset management is supported by documented procedures.	False
P1.4.1.5	All physical, software, and data assets are formally accounted for throughout the organization.	False
P1.4.1.7	The organization's inventory of information assets is centrally managed.	True
P1.5.1.3	Physical and logical access controls are integrated and adequately considered in policy.	True

P1.7.4.4	The scope of change management includes all necessary areas (equipment, operating systems, applications, documentation, etc.).	False
P3.8.3.3	Vulnerability scanning is conducted regularly, using tools separate from those used to remediate vulnerabilities.	False
P3.8.3.4	Validation processes are authenticated and running with sufficient privileges.	True
P4.1.3.9	Internet-facing systems are periodically audited for configuration changes and reconciled against change control documentation/evidence.	False

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

Statement	Statement Name	Status
P1.6.1.8	Encrypted data transfer solutions are provided to users (e.g., encrypted email, SFTP).	False
P1.7.11.1	Network security, including segregation and/or isolation of critical assets is a documented policy requirement.	False
P1.7.11.2	Network diagrams are available, are current, are sufficient in scope, and are sufficiently detailed.	True
P1.7.11.3	Data flow diagrams are available for all critical information assets, and they are sufficiently up to date, detailed, and scoped.	False
P1.7.15.2	The organization has developed and maintains a current inventory of all vendors, including purpose, scope, and information security risk requirements.	False
P1.7.4.4	The scope of change management includes all necessary areas (equipment, operating systems, applications, documentation, etc.).	False
P3.1.2.3	Egress and ingress traffic restrictions are in place and are limiting traffic to only what is required for operational purposes between WAN segments.	N/A
P3.1.3.3	Network segmentation is adequately leveraged to isolate and protect networked systems.	True
P3.1.3.6	Unmanaged network equipment (switches and hubs) is not employed for network connectivity; all network equipment is managed.	True
P3.2.1.2	The organization's remote access solution restricts the transfer of files through simple file sharing and mapping.	False
P4.1.3.1	Periodic scans for back-channel connections (those that bypass the DMZ) are conducted.	False
P4.1.3.2	External vulnerability scans are conducted on a quarterly basis, or more often.	False
P4.3.1.1	The organization regularly audits the ports that are open to the Internet.	False

Subcategory: ID.AM-4: External information systems are catalogued

Statement	Statement Name	Status
P1.4.1.6	Roles and responsibilities for developing and maintaining an inventory of information processing facilities and data assets are formally defined by management.	False
P1.7.11.2	Network diagrams are available, are current, are sufficient in scope, and are sufficiently detailed.	True
P1.7.11.6	Mechanisms such as secure gateway, VPN, routing, and switching technologies are implemented sufficiently to enable a graduated set of controls between different logical network domains and to segregate the network by security environments.	True
P1.7.11.8	Gateway devices are configured to filter traffic between domains and block unauthorized access in accordance with the organization's access control policy.	True
P1.7.15.2	The organization has developed and maintains a current inventory of all vendors, including purpose, scope, and information security risk requirements.	False
P4.1.3.1	Periodic scans for back-channel connections (those that bypass the DMZ) are conducted.	False
P4.1.3.2	External vulnerability scans are conducted on a quarterly basis, or more often.	False
P4.1.3.6	Web applications are tested for security on a regular basis.	True
P4.1.3.9	Internet-facing systems are periodically audited for configuration changes and reconciled against change control documentation/evidence.	False
P4.3.1.1	The organization regularly audits the ports that are open to the Internet.	False

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

Statement	Statement Name	Status
P1.7.11.7	Segregation of networks is based on the value and classification of information stored and/or processed in the network, levels of trust, lines of business, or need-to-know.	True
P1.7.15.3	Vendors as service providers are classified according to the inherent risk they pose to the organization.	True

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

Statement	Statement Name	Status
P1.1.1.4	Risk decisions (accept, mitigate, avoid, transfer, etc.) are made by executive management personnel with the authority to do so.	True
P1.10.2.5	A privacy officer (or equivalent) has been named and is known to all relevant personnel.	False
P1.10.4.2	Managers regularly review the level of compliance with information security policies and procedures within their respective areas of responsibility.	False
P1.2.2.3	The responsibilities for policy owners have been defined and documented.	True
P1.2.2.8	Management approval is required for all policy updates.	True
P1.4.1.6	Roles and responsibilities for developing and maintaining an inventory of information processing facilities and data assets are formally defined by management.	False
P1.5.1.2	The access control policy tasks asset owners with determining access control rules for the assets for which they are responsible.	False
P1.6.1.7	Roles and responsibilities for the implementation of an encryption policy and key management are defined by management.	False
P1.7.10.4	All information security audits are coordinated with and through system, application, and/or data owners.	False
P1.7.14.5	Testing results are formally accepted by system owners.	False
P1.7.15.8	third party contract oversight roles and responsibilities are defined and documented.	False
P1.7.4.5	Changes are properly justified and approved by management and information resource owners.	True

Business Environment (ID.BE)

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

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

Statement	Statement Name	Status
P3.9.3.1	Backups are taken in accordance with a documented disaster recovery and/or business continuity plan.	False
P3.9.3.2	Resilience requirements are documented and implemented in accordance with a business impact analysis.	False
P3.9.3.3	Backup data is encrypted while in storage and the encryption keys are accessible in a disaster situation.	False

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

Statement	Statement Name	Status
P1.1.1.9	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	False

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

Statement	Statement Name	Status
P1.1.1.2	Organizational risk tolerance is determined and clearly expressed (e.g., an acceptable risk score and/or risk threshold has been established, and defined criteria for which risks/risk levels require specific actions have been agreed upon).	False

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

Statement	Statement Name	Status
P2.3.1.1	Formal physical security policies and procedures exist, are up to date, and include the requirements for physical security and safety planning.	True
P2.3.4.4	Critical assets (people, activities, building systems and components) are not located close to a main entrance, vehicle circulation, parking, maintenance area, loading dock, and/or interior parking.	True
P2.4.2.1	Utility system design and physical security requirements are	True

	documented in policy and supporting procedures.	
P2.4.2.3	Uninterruptible power supplies (UPS) provide sufficient running time.	True
P2.4.2.4	A generator exists, is regularly tested, and has a fuel contract in place.	N/A
P2.4.2.8	Supporting utilities (e.g., electricity, telecommunications, water supply, gas, sewage, ventilation, air conditioning) are alarmed to detect malfunctions.	N/A
P2.4.2.9	All critical utility systems (e.g., electricity, telecommunications, water supply, gas, sewage, ventilation, and air conditioning) are secured.	True
P2.4.2.10	Utility systems and redundancies are tested on a regular basis.	False
P2.4.4.5	Management periodically performs maintenance and tests environmental controls (e.g., fire suppression systems, HVAC controls, power systems) to ensure operational availability.	True
P3.1.2.6	Critical business operations at secondary sites are supported by multiple redundant connections to the main site.	N/A

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

Statement	Statement Name	Status
P1.7.15.1	Formal policies and procedures to identify, evaluate, and manage risks associated with utilizing third party providers exist.	True
P1.9.2.1	The organization's recovery plans are likely to be executed appropriately during and after an event.	False
P1.9.2.2	The organization's recovery plans are tested on a periodic basis, and they have been tested within the past twelve (12) months.	False
P1.9.2.3	Recovery plans account for incorporating lessons learned during testing and after an event.	True
P1.9.2.4	Recovery strategies are updated to reflect the current operating environment.	True
P1.9.2.7	The recovery strategy is adequately communicated to all relevant internal personnel and executive management.	True
P3.9.2.1	Backup data storage is protected by strong encryption.	False
P3.9.2.2	Backup data is stored in a location that is sufficiently distanced from the primary operational facility.	False
P3.9.2.3	Storage capacity is sufficient to support backup data commensurate with business requirements.	False
P3.9.2.4	Backup data is transported to the storage environment in an encrypted form.	False

Governance (ID.GV)

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

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

Statement	Statement Name	Status
P1.10.2.1	A data policy for privacy and protection of personally identifiable information belonging to customers has been developed and adopted.	True
P1.10.2.2	A data policy for privacy and protection of personally identifiable information belonging to employees and contractors has been developed and adopted.	True
P1.10.5.1	Information security policies and procedures that are specific to financial systems exist.	False
P1.2.2.1	The management approval process for information security policies is well-defined and documented.	True
P1.2.2.4	Policies are consistently reviewed at planned intervals according to a defined schedule.	False
P1.2.2.5	Significant changes within the organization trigger policy reviews and updates.	False
P1.2.2.6	The criteria to be used during information security policy reviews has been formally defined.	True
P1.2.2.7	Information security policies have been formally reviewed within the last twelve months or less.	False
P1.4.1.1	An asset management (or similar) policy has been developed and is sufficient in scope.	True
P1.5.1.1	An access control policy has been documented and approved by senior management.	False
P1.5.2.1	User registration and de-registration practices are carried out in accordance with a documented policy.	True
P1.6.1.1	A policy for cryptographic controls has been developed and implemented by the organization.	True
P1.7.10.1	The organization's information security audit requirements are formally documented in policy or procedure.	False
P1.7.11.1	Network security, including segregation and/or isolation of critical assets is a documented policy requirement.	False
P1.7.15.1	Formal policies and procedures to identify, evaluate, and manage risks associated with utilizing third party providers exist.	True
P1.7.4.1	The organization has documented and adopted a formal change control (or similar) policy.	True
P2.3.1.1	Formal physical security policies and procedures exist, are up to date, and include the requirements for physical security	True

	and safety planning.	
P2.3.7.1	Formal policies and procedures for handling all deliveries are documented.	True
P2.4.2.1	Utility system design and physical security requirements are documented in policy and supporting procedures.	True
P2.4.4.1	Equipment maintenance security requirements are documented in policy and supported by procedures.	True
P2.4.6.1	Documented policy and procedures adequately define clear desk and clear screen requirements for securing sensitive and critical business information during and after work hours.	N/A

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

Statement	Statement Name	Status
P1.2.2.2	Policy owners have been identified and documented for all information security policies.	True
P1.2.2.3	The responsibilities for policy owners have been defined and documented.	True
P1.2.2.8	Management approval is required for all policy updates.	True
P1.7.15.8	third party contract oversight roles and responsibilities are defined and documented.	False
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False

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

Statement	Statement Name	Status
P1.10.1.1	All relevant statutory, regulatory, and contractual requirements have been explicitly defined and documented (e.g., GDPR, state breach notification laws, Massachusetts state law, HIPAA, GLBA, PCI, et al.).	True
P1.10.1.2	Legal and regulatory requirements regarding information security, including privacy and civil liberties obligation, are well-understood and managed.	True
P1.10.1.3	The organization is compliant with the General Data Protection Regulation (GDPR) when it should be.	N/A
P1.10.1.4	The organization is compliant with the Payment Card Industry Data Security Standard (PCI DSS) when it should be.	N/A
P1.10.1.5	The organization is compliant with the Health Insurance Portability and Accountability Act (HIPAA) when it should be.	True

P1.10.1.6	Advice on specific legal requirements has been sought from qualified legal counsel in an effort to protect the company from information security-related legal issues.	True
P1.10.2.3	The organization's privacy requirements have been formally communicated to all personnel involved in the processing of personally identifiable information.	True
P1.3.1.7	Background checks are performed in accordance with relevant state and federal laws regarding privacy and protection of information.	True
P1.3.3.6	The organization's information security awareness program includes key elements such as management's commitment to information security, complying with security requirements, legal responsibilities, basic security procedures, and key contact points (for incident reporting and additional information).	True
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False
P2.4.2.2	Fire suppression systems are adequate, code-compliant, and protected (within a secure location).	True

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

Statement	Statement Name	Status
P1.1.1.1	Risk management processes are formally established, managed, and agreed to by organizational stakeholders.	True
P1.1.1.3	The organization's risk management function provides consistent and actionable information for executive management decision-making.	True
P1.1.1.4	Risk decisions (accept, mitigate, avoid, transfer, etc.) are made by executive management personnel with the authority to do so.	True
P1.1.1.7	The organization's approach to Information security risk management is comprehensive; accounting for administrative (people), physical, and technical threats and vulnerabilities.	True
P1.1.1.8	The definition of "information security" and "risk" is well-understood, documented, and accurate.	False
P1.1.2.1	The organization has transferred information security risk by obtaining insurance.	True
P1.1.2.5	Key exclusions and/or sublimits included in insurance policies are well-understood and formally accounted for in policy or other related plans.	False
P1.10.4.1	Managers actively participate in the development and improvement of the information security program.	True

P1.10.4.2	Managers regularly review the level of compliance with information security policies and procedures within their respective areas of responsibility.	False
P4.1.3.10	Decision-making criteria and approval for risks and vulnerabilities are documented and followed.	True

Risk Assessment (ID.RA)

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

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

Statement	Statement Name	Status
P1.1.1.7	The organization's approach to Information security risk management is comprehensive; accounting for administrative (people), physical, and technical threats and vulnerabilities.	True
P1.7.15.7	Inherent and residual risk assessments for vendors and third party service providers sufficiently account for administrative, physical, and technical threats and vulnerabilities.	False
P3.8.3.1	The effectiveness of vulnerability management practices is validated on a periodic basis.	True
P3.8.3.3	Vulnerability scanning is conducted regularly, using tools separate from those used to remediate vulnerabilities.	False
P4.1.3.2	External vulnerability scans are conducted on a quarterly basis, or more often.	False

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

Statement	Statement Name	Status
P1.1.1.6	Threats, both internal and external, are identified and documented as part of the risk management practice.	True

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

Statement	Statement Name	Status
P1.1.1.6	Threats, both internal and external, are identified and documented as part of the risk management practice.	True
P1.1.1.7	The organization's approach to Information security risk management is comprehensive; accounting for administrative (people), physical, and technical threats and vulnerabilities.	True
P1.3.3.7	Updates to information security policies and practices, and new vulnerabilities and threats are communicated to employees, contractors, and third party resources in a timely manner.	False
P1.7.15.7	Inherent and residual risk assessments for vendors and third party service providers sufficiently account for administrative, physical, and technical threats and vulnerabilities.	False
P2.3.7.8	Incoming materials are registered, isolated, and inspected for	True

	potential threats prior to being moved to more internal areas.	

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

Statement	Statement Name	Status
P1.1.1.5	Risk decisions are identified and prioritized according to defined criteria.	True
P1.1.1.8	The definition of "information security" and "risk" is well-understood, documented, and accurate.	False
P1.7.4.3	The organization's change management processes include all necessary elements (identifying and recording changes, planning, and testing changes, assessment of potential impacts including security impacts, formal approval procedure, communication of change details, back-out plan, etc.).	True
P1.9.2.6	Strategies to address and limit the reputational impact from an event are formally accounted for.	True
P3.9.3.2	Resilience requirements are documented and implemented in accordance with a business impact analysis.	False

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

Statement	Statement Name	Status
P1.1.1.1	Risk management processes are formally established, managed, and agreed to by organizational stakeholders.	True
P1.1.1.5	Risk decisions are identified and prioritized according to defined criteria.	True
P1.1.1.6	Threats, both internal and external, are identified and documented as part of the risk management practice.	True
P1.1.1.7	The organization's approach to Information security risk management is comprehensive; accounting for administrative (people), physical, and technical threats and vulnerabilities.	True
P1.1.1.8	The definition of "information security" and "risk" is well-understood, documented, and accurate.	False

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

Statement	Statement Name	Status
P1.1.1.3	The organization's risk management function provides consistent and actionable information for executive management decision-making.	True
P1.1.1.4	Risk decisions (accept, mitigate, avoid, transfer, etc.) are	True

	made by executive management personnel with the authority to do so.	
P1.1.1.5	Risk decisions are identified and prioritized according to defined criteria.	True

Risk Management Strategy (ID.RM)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

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

Statement	Statement Name	Status
P1.1.1.1	Risk management processes are formally established, managed, and agreed to by organizational stakeholders.	True
P1.1.1.2	Organizational risk tolerance is determined and clearly expressed (e.g., an acceptable risk score and/or risk threshold has been established, and defined criteria for which risks/risk levels require specific actions have been agreed upon).	False
P1.1.1.5	Risk decisions are identified and prioritized according to defined criteria.	True
P1.1.1.8	The definition of "information security" and "risk" is well-understood, documented, and accurate.	False
P1.1.1.9	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	False
P1.1.2.1	The organization has transferred information security risk by obtaining insurance.	True
P4.1.3.10	Decision-making criteria and approval for risks and vulnerabilities are documented and followed.	True

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

Statement	Statement Name	Status
P1.1.1.2	Organizational risk tolerance is determined and clearly expressed (e.g., an acceptable risk score and/or risk threshold has been established, and defined criteria for which risks/risk levels require specific actions have been agreed upon).	False
P1.1.1.5	Risk decisions are identified and prioritized according to defined criteria.	True
P1.1.1.8	The definition of "information security" and "risk" is well-understood, documented, and accurate.	False
P1.1.1.9	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	False

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

Statement	Statement Name	Status
P1.1.1.9	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	False

Supply Chain Risk Management (ID.SC)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Subcategory: ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

Statement	Statement Name	Status
P1.3.3.7	Updates to information security policies and practices, and new vulnerabilities and threats are communicated to employees, contractors, and third party resources in a timely manner.	False
P1.7.15.1	Formal policies and procedures to identify, evaluate, and manage risks associated with utilizing third party providers exist.	True
P1.7.15.5	Inherent and residual risks related to vendor and third party relationships are reviewed on a regular and ongoing basis.	True
P1.7.15.8	third party contract oversight roles and responsibilities are defined and documented.	False
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False

Subcategory: ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

Statement	Statement Name	Status
P1.1.1.1	Risk management processes are formally established, managed, and agreed to by organizational stakeholders.	True
P1.7.15.2	The organization has developed and maintains a current inventory of all vendors, including purpose, scope, and information security risk requirements.	False
P1.7.15.3	Vendors as service providers are classified according to the inherent risk they pose to the organization.	True
P1.7.15.4	Higher inherent risk vendors are subjected to more scrutiny, including formalized and more comprehensive residual risk assessments.	True
P1.7.15.5	Inherent and residual risks related to vendor and third party relationships are reviewed on a regular and ongoing basis.	True
P1.7.15.6	Residual risks related to the highest risk vendors and third party service providers are validated.	True
P1.7.15.7	Inherent and residual risk assessments for vendors and third	False

	party service providers sufficiently account for administrative, physical, and technical threats and vulnerabilities.	
P1.7.15.8	third party contract oversight roles and responsibilities are defined and documented.	False
P1.7.15.9	Procedures to handle information security incidents and provide continuation of third party access in the event of an information security incident are defined.	False
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False

Subcategory: ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

Statement	Statement Name	Status
P1.10.2.2	A data policy for privacy and protection of personally identifiable information belonging to employees and contractors has been developed and adopted.	True
P1.7.15.8	third party contract oversight roles and responsibilities are defined and documented.	False
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False

Subcategory: ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

Statement	Statement Name	Status
P1.7.10.2	Periodic audits for compliance with information security requirements are performed according to a defined schedule.	False
P1.7.10.3	Access control audits (user accounts, rights, privileges, and other access) are performed on a regular basis.	False
P1.7.15.5	Inherent and residual risks related to vendor and third party relationships are reviewed on a regular and ongoing basis.	True
P1.7.15.6	Residual risks related to the highest risk vendors and third party service providers are validated.	True
P1.7.15.8	third party contract oversight roles and responsibilities are defined and documented.	False
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False

Subcategory: ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

Statement	Statement Name	Status
P1.3.3.3	Employees, contractors, and third party resources receive security awareness training prior to being granted access to information resources.	False
P1.3.3.4	Employees, contractors, and third party resources receive security awareness training on a periodic basis.	False
P1.3.3.7	Updates to information security policies and practices, and new vulnerabilities and threats are communicated to employees, contractors, and third party resources in a timely manner.	False
P1.7.14.3	New information systems, upgrades and new versions are implemented with formal information security testing.	False
P1.7.15.9	Procedures to handle information security incidents and provide continuation of third party access in the event of an information security incident are defined.	False
P1.9.2.2	The organization's recovery plans are tested on a periodic basis, and they have been tested within the past twelve (12) months.	False
P2.3.1.6	Facility evacuation procedures are documented, posted, and tested.	True
P2.4.2.10	Utility systems and redundancies are tested on a regular basis.	False
P2.4.4.5	Management periodically performs maintenance and tests environmental controls (e.g., fire suppression systems, HVAC controls, power systems) to ensure operational availability.	True

PROTECT Function

Access Control	Awareness and Training	Data Security
691	583	637
Information Protection	**Maintenance**	**Protective Technology**
616	662	643

NIST CSF PROTECT Function includes the following Categories:

- **Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- **Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
- **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
- **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Access Control (PR.AC)

Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

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

Statement	Statement Name	Status
P1.10.5.6	The use of strong authentication is required for all access to financial systems.	True
P1.5.1.1	An access control policy has been documented and approved by senior management.	False
P1.5.1.8	A periodic review of user accounts and access rights is conducted according to a defined process and procedure.	True
P1.5.2.1	User registration and de-registration practices are carried out in accordance with a documented policy.	True
P1.5.2.2	The organization has adopted formalized procedures for the creation, enablement, modification, disablement, and removal of all information resource accounts.	True
P1.5.2.3	All user account management activities are formally authorized and documented to a level that provides an audit trail.	True
P1.5.2.4	Procedures for system account usage are documented and followed.	True
P1.5.2.5	The use of shared user accounts is prohibited by the organization.	True
P1.5.2.6	User de-registration processes adequately ensure that user accounts are disabled or removed immediately after a user leaves the organization.	True
P1.5.2.7	User account review/audit processes are implemented to identify and disable (or remove) redundant user accounts.	False
P1.5.2.8	System/service accounts are inventoried and specifically authorized.	False
P1.7.10.3	Access control audits (user accounts, rights, privileges, and other access) are performed on a regular basis.	False
P2.3.4.2	Access control is provided through all main entrance points used by employees and visitors (lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems).	True
P2.3.5.7	The identity of visitors is authenticated.	True
P3.2.1.1	Multi-factor authentication is used for all client remote access to the organization's network(s).	True
P3.7.4.2	The credentials (username/password) used for day-to-day management of information systems is different than the credentials for managing the organization's logging systems.	False

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

Statement	Statement Name	Status
P2.3.1.1	Formal physical security policies and procedures exist, are up to date, and include the requirements for physical security and safety planning.	True
P2.3.1.3	Facility physical security risk assessments and security audits are conducted on a regular basis.	False
P2.3.1.7	Facility security is formally incorporated into an employee training program.	True
P2.3.1.9	Security guards are employed and are formally trained and tested on all facility security and emergency response procedures.	N/A
P2.3.4.1	Physical security controls are implemented to properly secure and segregate facilities where multiple organizations are doing business (or where IT assets are managed by third party resources).	True
P2.3.4.2	Access control is provided through all main entrance points used by employees and visitors (lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems).	True
P2.3.4.3	Public and private areas within the facility are adequately separated, for instance public access to toilets, service spaces, access to public stairways, and/or elevators are not provided within private areas.	False
P2.3.4.4	Critical assets (people, activities, building systems and components) are not located close to a main entrance, vehicle circulation, parking, maintenance area, loading dock, and/or interior parking.	True
P2.3.4.5	A manned reception area or other means to control physical access to the site or building is in place.	True
P2.3.4.7	The approach to loitering is defined and communicated to all relevant parties.	True
P2.3.4.8	Public spaces are covered by camera surveillance.	False
P2.3.4.9	Activities occurring within public spaces are actively monitored.	True
P2.3.5.1	Access to office spaces is sufficiently segregated from public spaces.	True
P2.3.5.2	Employees, contractors, and external parties are required to wear some form of visible identification.	False
P2.3.5.3	The date and time of entry and departure of visitors is recorded.	True
P2.3.5.4	Visitors are escorted and always supervised while visiting non-public areas of the facility.	True

P2.3.5.5	Visitors are only granted access for specific and authorized purposes.	True
P2.3.5.6	Visitors are informed of specific facility security requirements and emergency procedures.	True
P2.3.5.7	The identity of visitors is authenticated.	True
P2.3.5.8	Employees, contractors, and external parties have been instructed to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.	True
P2.3.5.9	Access rights to office spaces areas are regularly reviewed and updated (or revoked) when necessary.	True
P2.3.5.10	All exits have a card-in/card-out audit trail or security cameras cover all exits.	True
P2.3.7.1	Formal policies and procedures for handling all deliveries are documented.	True
P2.3.7.2	A response checklist for suspicious persons and packages has been created and followed.	True
P2.3.7.3	Doors to public areas (e.g., receptions, delivery, and loading dock) are locked and secured.	True
P2.3.7.4	External doors of delivery and loading areas are secured when the internal doors are opened.	True
P2.3.7.5	Public, delivery, and loading areas are staffed.	True
P2.3.7.6	Public, delivery, and loading areas are covered by surveillance cameras (CCTV).	False
P2.3.7.7	There is a second (internal) physically locked partition to separate public, delivery, and loading areas from rest of the internal facilities.	False
P2.3.7.8	Incoming materials are registered, isolated, and inspected for potential threats prior to being moved to more internal areas.	True
P2.3.7.9	Incoming materials are inspected for evidence of tampering and if tampering is discovered it is immediately reported to security personnel.	True
P2.3.7.10	Incoming and outgoing activities occur in separate physical areas.	False
P2.4.4.1	Equipment maintenance security requirements are documented in policy and supported by procedures.	True
P2.4.4.4	Records are kept of preventive and corrective equipment maintenance activities.	True

Subcategory: PR.AC-3: Remote access is managed

Statement	Statement Name	Status
P3.1.2.1	Firewalls (or other packet filtering and control devices) are	N/A

	used to secure traffic between networks at remote sites.	
P3.1.2.2	Systems at remote sites are unable to access untrusted networks (e.g., the Internet) without passing through firewalls (or other packet filtering and control devices).	N/A
P3.1.2.3	Egress and ingress traffic restrictions are in place and are limiting traffic to only what is required for operational purposes between WAN segments.	N/A
P3.1.2.4	Traffic between sites is adequately protected from eavesdropping.	N/A
P3.1.2.5	Network security controls employed at remote sites are the same as, or similar to, those used at the main site.	N/A
P3.2.1.1	Multi-factor authentication is used for all client remote access to the organization's network(s).	True
P3.2.1.2	The organization's remote access solution restricts the transfer of files through simple file sharing and mapping.	False
P3.2.1.3	Remote access traffic is sufficiently encrypted.	True
P3.2.1.4	Remote access traffic is properly segmented from internal trusted networks.	False
P3.2.1.5	The organization consistently monitors remote access connection attempts and traffic.	False
P3.2.1.6	Remote access is only provided to users who specifically require the privilege.	True
P3.2.1.7	Remote access rights are periodically reviewed and reconciled.	True

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

Statement	Statement Name	Status
P1.10.5.4	Dual control is required on all financial transactions exceeding certain dollar amounts.	False
P1.10.5.5	Dual control is required for all changes to payment accounts and all payment account setups.	True
P1.5.1.1	An access control policy has been documented and approved by senior management.	False
P1.5.1.2	The access control policy tasks asset owners with determining access control rules for the assets for which they are responsible.	False
P1.5.1.3	Physical and logical access controls are integrated and adequately considered in policy.	True
P1.5.1.4	The access control policy accounts for information dissemination in accordance with the need-to-know principle and data classification.	False
P1.5.1.5	The access control policy and supporting documentation adequately addresses the management of access rights (e.g.,	True

	access provisioning, access management/changes, and access revocation).	
P1.5.1.6	Segregation of access control roles is sufficient (e.g., access request, access authorization, and access administration).	True
P1.5.1.7	The access control policy requires and addresses the formal authorization of all access requests.	True
P1.5.1.9	The rules governing roles with privileged access are documented and consistently followed.	True
P1.5.1.10	Access rights are linked and integrated with specific business roles (role-based access control).	True
P1.7.10.3	Access control audits (user accounts, rights, privileges, and other access) are performed on a regular basis.	False
P1.7.14.8	Developers and/or non-admin personnel do not maintain standing back end access to production systems.	False
P2.3.5.5	Visitors are only granted access for specific and authorized purposes.	True
P2.3.5.9	Access rights to office spaces areas are regularly reviewed and updated (or revoked) when necessary.	True
P3.2.1.6	Remote access is only provided to users who specifically require the privilege.	True
P3.2.1.7	Remote access rights are periodically reviewed and reconciled.	True
P3.6.1.1	A mobile device management solution is used to enforce consistent control for all mobile devices with access to non-public organizational information.	False
P3.8.3.4	Validation processes are authenticated and running with sufficient privileges.	True

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

Statement	Statement Name	Status
P1.6.1.8	Encrypted data transfer solutions are provided to users (e.g., encrypted email, SFTP).	False
P1.7.11.1	Network security, including segregation and/or isolation of critical assets is a documented policy requirement.	False
P1.7.11.2	Network diagrams are available, are current, are sufficient in scope, and are sufficiently detailed.	True
P1.7.11.3	Data flow diagrams are available for all critical information assets, and they are sufficiently up to date, detailed, and scoped.	False
P1.7.11.4	Internal penetration testing is conducted to ensure that controls are operating as intended, and that lateral movement within the organization's networks is sufficiently controlled.	True

P1.7.11.5	Risk assessments are conducted to determine requirements for the implementation of graduated controls that segregate different logical network domains (e.g., publicly accessible systems, internal networks, and critical assets) and security environments.	True
P1.7.11.6	Mechanisms such as secure gateway, VPN, routing, and switching technologies are implemented sufficiently to enable a graduated set of controls between different logical network domains and to segregate the network by security environments.	True
P1.7.11.7	Segregation of networks is based on the value and classification of information stored and/or processed in the network, levels of trust, lines of business, or need-to-know.	True
P1.7.11.8	Gateway devices are configured to filter traffic between domains and block unauthorized access in accordance with the organization's access control policy.	True
P1.7.11.9	The development and testing environment(s) are network-isolated from the production environment.	True
P3.1.2.1	Firewalls (or other packet filtering and control devices) are used to secure traffic between networks at remote sites.	N/A
P3.1.2.3	Egress and ingress traffic restrictions are in place and are limiting traffic to only what is required for operational purposes between WAN segments.	N/A
P3.1.3.1	Switch ports are only active when necessary and approved; otherwise, the ports are disabled or secured using other means.	True
P3.1.3.2	The organization leverages port-based network access control (802.1x).	False
P3.1.3.3	Network segmentation is adequately leveraged to isolate and protect networked systems.	True
P3.1.3.4	The organization has implemented a separate, isolated management network.	True
P3.1.3.6	Unmanaged network equipment (switches and hubs) is not employed for network connectivity; all network equipment is managed.	True
P3.1.3.8	Security-specific systems are deployed on a dedicated network subnet.	True
P3.2.1.2	The organization's remote access solution restricts the transfer of files through simple file sharing and mapping.	False
P3.2.1.4	Remote access traffic is properly segmented from internal trusted networks.	False
P4.1.3.1	Periodic scans for back-channel connections (those that bypass the DMZ) are conducted.	False
P4.3.1.1	The organization regularly audits the ports that are open to the Internet.	False

Subcategory: PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions

Statement	Statement Name	Status
P1.5.1.1	An access control policy has been documented and approved by senior management.	False
P1.5.1.2	The access control policy tasks asset owners with determining access control rules for the assets for which they are responsible.	False
P1.5.1.6	Segregation of access control roles is sufficient (e.g., access request, access authorization, and access administration).	True
P1.5.2.1	User registration and de-registration practices are carried out in accordance with a documented policy.	True
P1.5.2.2	The organization has adopted formalized procedures for the creation, enablement, modification, disablement, and removal of all information resource accounts.	True
P1.5.2.3	All user account management activities are formally authorized and documented to a level that provides an audit trail.	True
P1.5.2.5	The use of shared user accounts is prohibited by the organization.	True
P1.5.2.8	System/service accounts are inventoried and specifically authorized.	False
P2.3.4.2	Access control is provided through all main entrance points used by employees and visitors (lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems).	True
P2.3.5.3	The date and time of entry and departure of visitors is recorded.	True
P2.3.5.7	The identity of visitors is authenticated.	True
P3.2.1.1	Multi-factor authentication is used for all client remote access to the organization's network(s).	True

Subcategory: PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

Statement	Statement Name	Status
P1.10.5.6	The use of strong authentication is required for all access to financial systems.	True
P2.3.5.7	The identity of visitors is authenticated.	True
P3.2.1.1	Multi-factor authentication is used for all client remote access to the organization's network(s).	True
P3.6.1.4	The mobile devices that could contain sensitive information are protected with enforced authentication.	True
P4.3.1.6	Administrative login pages are secured with multi-factor	False

	authentication.	
P4.3.1.7	General-user login pages are secured with multi-factor authentication.	False

Awareness and Training (PR.AT)

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

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

Statement	Statement Name	Status
P1.3.3.1	The organization has developed a formal information security awareness, education, and training program.	True
P1.3.3.2	Information security awareness, education, and training is mandated in policy.	True
P1.3.3.3	Employees, contractors, and third party resources receive security awareness training prior to being granted access to information resources.	False
P1.3.3.4	Employees, contractors, and third party resources receive security awareness training on a periodic basis.	False
P1.3.3.5	Role-specific information security education has been formalized and delivered.	False
P1.3.3.6	The organization's information security awareness program includes key elements such as management's commitment to information security, complying with security requirements, legal responsibilities, basic security procedures, and key contact points (for incident reporting and additional information).	True
P1.3.3.7	Updates to information security policies and practices, and new vulnerabilities and threats are communicated to employees, contractors, and third party resources in a timely manner.	False
P1.3.3.8	The effectiveness of information security training and awareness exercises is measured in a quantifiable manner.	False
P1.6.1.10	Users are formally trained on the use and importance of data encryption to protect the confidentiality and integrity of information.	False
P2.3.1.7	Facility security is formally incorporated into an employee training program.	True
P2.3.5.6	Visitors are informed of specific facility security requirements and emergency procedures.	True
P2.4.6.2	User awareness training provides guidance on clear desk and clear screen requirements.	N/A

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

Statement	Statement Name	Status
P1.10.5.2	Personnel with access to financial systems receive role-specific training about financial fraud.	False
P1.5.1.9	The rules governing roles with privileged access are documented and consistently followed.	True

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

Statement	Statement Name	Status
P1.3.3.3	Employees, contractors, and third party resources receive security awareness training prior to being granted access to information resources.	False
P1.3.3.4	Employees, contractors, and third party resources receive security awareness training on a periodic basis.	False
P1.3.3.7	Updates to information security policies and practices, and new vulnerabilities and threats are communicated to employees, contractors, and third party resources in a timely manner.	False

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

Statement	Statement Name	Status
P1.1.1.4	Risk decisions (accept, mitigate, avoid, transfer, etc.) are made by executive management personnel with the authority to do so.	True
P1.9.2.7	The recovery strategy is adequately communicated to all relevant internal personnel and executive management.	True

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

Statement	Statement Name	Status
P1.10.2.5	A privacy officer (or equivalent) has been named and is known to all relevant personnel.	False
P2.3.1.1	Formal physical security policies and procedures exist, are up to date, and include the requirements for physical security and safety planning.	True
P2.3.1.9	Security guards are employed and are formally trained and tested on all facility security and emergency response procedures.	N/A
P2.3.5.8	Employees, contractors, and external parties have been instructed to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible	True

	identification.	
P2.4.4.2	Maintenance is performed by personnel who have received specialized training.	True

Data Security (PR.DS)

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

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

Statement	Statement Name	Status
P1.4.1.5	All physical, software, and data assets are formally accounted for throughout the organization.	False
P1.6.1.1	A policy for cryptographic controls has been developed and implemented by the organization.	True
P1.6.1.2	Management's approach to encryption and the general principles by which information must be encrypted are documented.	True
P1.6.1.3	Use and deployment of encryption is based on a risk assessment, accounting for required levels of protection, key strength, and quality of the encryption algorithm.	False
P1.6.1.4	Encryption requirements for protecting data at rest are documented.	False
P1.6.1.6	Policies and procedures around key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case they are lost, compromised, or damaged, are defined.	False
P1.6.1.7	Roles and responsibilities for the implementation of an encryption policy and key management are defined by management.	False
P1.6.1.9	The loss of cryptographic keys or other compromise of encryption is accounted for in the organization's incident response processes.	False
P1.6.1.10	Users are formally trained on the use and importance of data encryption to protect the confidentiality and integrity of information.	False
P2.3.1.1	Formal physical security policies and procedures exist, are up to date, and include the requirements for physical security and safety planning.	True
P3.6.1.3	Encryption is used to protect information on mobile devices.	True
P3.9.2.1	Backup data storage is protected by strong encryption.	False
P3.9.3.3	Backup data is encrypted while in storage and the encryption keys are accessible in a disaster situation.	False

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

Statement	Statement Name	Status

P1.6.1.1	A policy for cryptographic controls has been developed and implemented by the organization.	True
P1.6.1.2	Management's approach to encryption and the general principles by which information must be encrypted are documented.	True
P1.6.1.3	Use and deployment of encryption is based on a risk assessment, accounting for required levels of protection, key strength, and quality of the encryption algorithm.	False
P1.6.1.5	Encryption requirements for protecting data in transit are documented.	False
P1.6.1.6	Policies and procedures around key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case they are lost, compromised, or damaged, are defined.	False
P1.6.1.7	Roles and responsibilities for the implementation of an encryption policy and key management are defined by management.	False
P1.6.1.8	Encrypted data transfer solutions are provided to users (e.g., encrypted email, SFTP).	False
P1.6.1.9	The loss of cryptographic keys or other compromise of encryption is accounted for in the organization's incident response processes.	False
P1.6.1.10	Users are formally trained on the use and importance of data encryption to protect the confidentiality and integrity of information.	False
P1.7.11.3	Data flow diagrams are available for all critical information assets, and they are sufficiently up to date, detailed, and scoped.	False
P3.1.2.4	Traffic between sites is adequately protected from eavesdropping.	N/A
P3.2.1.3	Remote access traffic is sufficiently encrypted.	True
P3.6.1.7	Encryption is employed when using mobile devices to connect to organizational resources.	True
P3.9.2.4	Backup data is transported to the storage environment in an encrypted form.	False

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

Statement	Statement Name	Status
P1.4.1.1	An asset management (or similar) policy has been developed and is sufficient in scope.	True
P1.4.1.2	Physical devices and systems within the organization are all inventoried.	True
P1.4.1.3	Software platforms and applications within the organization are inventoried.	False

P1.4.1.4	Asset management is supported by documented procedures.	False
P1.4.1.5	All physical, software, and data assets are formally accounted for throughout the organization.	False
P1.4.1.6	Roles and responsibilities for developing and maintaining an inventory of information processing facilities and data assets are formally defined by management.	False
P1.4.1.8	Formal asset reconciliation processes are sufficient to account for lost, damaged, and stolen assets.	False
P1.4.1.9	The organization's asset management practices account for the entire asset life-cycle.	True
P2.3.4.8	Public spaces are covered by camera surveillance.	False
P2.3.4.9	Activities occurring within public spaces are actively monitored.	True
P2.3.5.3	The date and time of entry and departure of visitors is recorded.	True
P2.3.5.7	The identity of visitors is authenticated.	True
P2.3.5.10	All exits have a card-in/card-out audit trail or security cameras cover all exits.	True
P2.3.7.5	Public, delivery, and loading areas are staffed.	True
P2.3.7.6	Public, delivery, and loading areas are covered by surveillance cameras (CCTV).	False

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

Statement	Statement Name	Status
P1.7.3.6	In the event of unexpected operational or technical difficulties, support, and escalation contacts (including external support contacts) are documented.	True
P2.4.2.2	Fire suppression systems are adequate, code-compliant, and protected (within a secure location).	True
P2.4.2.3	Uninterruptible power supplies (UPS) provide sufficient running time.	True
P2.4.2.4	A generator exists, is regularly tested, and has a fuel contract in place.	N/A
P2.4.4.5	Management periodically performs maintenance and tests environmental controls (e.g., fire suppression systems, HVAC controls, power systems) to ensure operational availability.	True
P3.4.3.2	The storage environment is supported by an appropriate level of redundancy (e.g., local, SAN, NFS, iSCSI).	True
P3.4.3.3	The storage environment has the appropriate capacity and ability to expand for the foreseeable needs (3-5 years).	True
P3.5.2.1	Workstations have sufficient capacity to support their operating requirements (e.g., RAM, Processor and Disk Space).	True

P3.9.2.3	Storage capacity is sufficient to support backup data commensurate with business requirements.	False

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

Statement	Statement Name	Status
P1.10.5.2	Personnel with access to financial systems receive role-specific training about financial fraud.	False
P1.7.11.2	Network diagrams are available, are current, are sufficient in scope, and are sufficiently detailed.	True
P1.7.11.3	Data flow diagrams are available for all critical information assets, and they are sufficiently up to date, detailed, and scoped.	False
P1.7.11.8	Gateway devices are configured to filter traffic between domains and block unauthorized access in accordance with the organization's access control policy.	True
P1.7.14.8	Developers and/or non-admin personnel do not maintain standing back end access to production systems.	False
P1.7.15.1	Formal policies and procedures to identify, evaluate, and manage risks associated with utilizing third party providers exist.	True
P3.1.2.3	Egress and ingress traffic restrictions are in place and are limiting traffic to only what is required for operational purposes between WAN segments.	N/A
P3.1.2.4	Traffic between sites is adequately protected from eavesdropping.	N/A
P3.1.3.1	Switch ports are only active when necessary and approved; otherwise, the ports are disabled or secured using other means.	True
P3.2.1.1	Multi-factor authentication is used for all client remote access to the organization's network(s).	True
P3.2.1.2	The organization's remote access solution restricts the transfer of files through simple file sharing and mapping.	False
P3.6.1.1	A mobile device management solution is used to enforce consistent control for all mobile devices with access to non-public organizational information.	False
P3.6.1.2	The organization enforces consistent control for any/all personally owned mobile devices that are permitted to access information.	False
P3.6.1.3	Encryption is used to protect information on mobile devices.	True
P3.6.1.4	The mobile devices that could contain sensitive information are protected with enforced authentication.	True
P3.6.1.5	Remote wipe capabilities are available and used to protect data on lost and/or stolen mobile devices.	True
P3.6.1.7	Encryption is employed when using mobile devices to	True

	connect to organizational resources.	
P4.1.3.2	External vulnerability scans are conducted on a quarterly basis, or more often.	False
P4.1.3.6	Web applications are tested for security on a regular basis.	True
P4.1.3.8	Penetration testing has been conducted against all externally facing systems in the past 12 months.	False
P4.1.3.9	Internet-facing systems are periodically audited for configuration changes and reconciled against change control documentation/evidence.	False
P4.2.1.1	The organization performs searches of the Internet on a regular basis, looking for sensitive information that may have been exposed.	False
P4.2.1.2	The organization performs searches of common social media sites on a regular basis, looking for sensitive information that may have been exposed.	False
P4.2.1.3	The organization performs searches of common file sharing sites on a regular basis, looking for sensitive information that may have been exposed.	False
P4.2.1.4	Sensitive information was not discovered in publicly accessible locations on one or more of the organization's Internet-accessible systems.	False
P4.2.1.5	No other publicly available information was discovered about the organization that could be valuable to an attacker.	True
P4.2.1.6	The organization has validated that DNS zone transfers are prohibited, except between primary and secondary servers.	True
P4.3.1.1	The organization regularly audits the ports that are open to the Internet.	False
P4.3.1.5	Public connections to administrative login pages are not permitted.	False
P4.3.1.6	Administrative login pages are secured with multi-factor authentication.	False
P4.3.1.7	General-user login pages are secured with multi-factor authentication.	False
P4.4.1.3	There are no known exploitable critical or high-severity vulnerabilities exposed to the Internet or any other public network.	False

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

Statement	Statement Name	Status
P1.10.5.4	Dual control is required on all financial transactions exceeding certain dollar amounts.	False
P1.10.5.5	Dual control is required for all changes to payment accounts and all payment account setups.	True

P1.10.5.6	The use of strong authentication is required for all access to financial systems.	True
P1.10.5.7	Financial accounts are monitored and balanced daily.	True
P1.6.1.10	Users are formally trained on the use and importance of data encryption to protect the confidentiality and integrity of information.	False
P1.7.10.3	Access control audits (user accounts, rights, privileges, and other access) are performed on a regular basis.	False
P1.7.14.1	The organization engages in software development with a documented and well-established secure software development lifecycle.	False
P1.7.4.2	Changes to the business processes, information processing facilities, and systems that affect information security are formally controlled.	True
P3.4.3.1	The organization regularly scans storage systems in search of unusual or unauthorized file storage.	True
P4.1.3.9	Internet-facing systems are periodically audited for configuration changes and reconciled against change control documentation/evidence.	False

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

Statement	Statement Name	Status
P1.7.11.5	Risk assessments are conducted to determine requirements for the implementation of graduated controls that segregate different logical network domains (e.g., publicly accessible systems, internal networks, and critical assets) and security environments.	True
P1.7.11.9	The development and testing environment(s) are network-isolated from the production environment.	True
P1.7.14.7	Testing is conducted in a test environment, separate from the production environment and the test environment closely resembles the production environment.	False
P1.7.14.9	There are formal procedures in place to ensure that the test environment closely resembles the final production environment.	False

Subcategory: PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity

Statement	Statement Name	Status
P1.4.1.2	Physical devices and systems within the organization are all inventoried.	True
P1.7.4.4	The scope of change management includes all necessary	False

	areas (equipment, operating systems, applications, documentation, etc.).	
P1.7.4.6	Changes are tracked and reviewed; audits of system maintenance activities are being performed.	False
P2.4.4.1	Equipment maintenance security requirements are documented in policy and supported by procedures.	True
P2.4.4.2	Maintenance is performed by personnel who have received specialized training.	True
P2.4.4.3	Records are kept for suspected and actual faults (i.e., system problems).	True
P2.4.4.4	Records are kept of preventive and corrective equipment maintenance activities.	True
P2.4.4.5	Management periodically performs maintenance and tests environmental controls (e.g., fire suppression systems, HVAC controls, power systems) to ensure operational availability.	True

Information Protection Processes and Procedures (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

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

Statement	Statement Name	Status
P1.4.1.9	The organization's asset management practices account for the entire asset life-cycle.	True
P1.7.3.2	Documented operating procedures for the installation and configuration of server systems exist and are followed.	True
P1.7.3.3	Documented operating procedures for the installation and configuration of client systems exist and are followed.	True
P4.1.3.9	Internet-facing systems are periodically audited for configuration changes and reconciled against change control documentation/evidence.	False

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

Statement	Statement Name	Status
P1.7.14.1	The organization engages in software development with a documented and well-established secure software development lifecycle.	False
P1.7.14.2	Formal acceptance testing criteria have been defined and documented for new information systems, upgrades, and versions.	False
P1.7.14.3	New information systems, upgrades and new versions are implemented with formal information security testing.	False
P1.7.14.4	The types of testing are adequate for new systems, upgrades, and versions.	False
P1.7.14.5	Testing results are formally accepted by system owners.	False
P1.7.14.6	Automated tools are leveraged for testing information systems, upgrades, and new versions.	False
P1.7.14.7	Testing is conducted in a test environment, separate from the production environment and the test environment closely resembles the production environment.	False
P1.7.14.8	Developers and/or non-admin personnel do not maintain standing back end access to production systems.	False
P1.7.14.9	There are formal procedures in place to ensure that the test environment closely resembles the final production environment.	False

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

Statement	Statement Name	Status
P1.10.5.5	Dual control is required for all changes to payment accounts and all payment account setups.	True
P1.7.3.2	Documented operating procedures for the installation and configuration of server systems exist and are followed.	True
P1.7.3.3	Documented operating procedures for the installation and configuration of client systems exist and are followed.	True
P1.7.4.1	The organization has documented and adopted a formal change control (or similar) policy.	True
P1.7.4.2	Changes to the business processes, information processing facilities, and systems that affect information security are formally controlled.	True
P1.7.4.3	The organization's change management processes include all necessary elements (identifying and recording changes, planning, and testing changes, assessment of potential impacts including security impacts, formal approval procedure, communication of change details, back-out plan, etc.).	True
P1.7.4.4	The scope of change management includes all necessary areas (equipment, operating systems, applications, documentation, etc.).	False
P1.7.4.5	Changes are properly justified and approved by management and information resource owners.	True
P1.7.4.6	Changes are tracked and reviewed; audits of system maintenance activities are being performed.	False
P4.1.3.7	Web applications are tested for security each time a change is made.	N/A
P4.1.3.9	Internet-facing systems are periodically audited for configuration changes and reconciled against change control documentation/evidence.	False

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

Statement	Statement Name	Status
P1.7.3.4	Detailed operating procedures and instructions for backups are documented, reviewed, and kept up to date.	True
P1.7.3.7	Operating procedures are complete and comprehensive to include the proper level of detail (i.e., they include processing and handling, backup, interdependencies with other systems and scheduling requirements, error handling and exceptional conditions, support contacts, system restart and recovery steps, etc.).	False

P3.9.2.1	Backup data storage is protected by strong encryption.	False
P3.9.2.2	Backup data is stored in a location that is sufficiently distanced from the primary operational facility.	False
P3.9.2.3	Storage capacity is sufficient to support backup data commensurate with business requirements.	False
P3.9.2.4	Backup data is transported to the storage environment in an encrypted form.	False
P3.9.3.1	Backups are taken in accordance with a documented disaster recovery and/or business continuity plan.	False
P3.9.3.3	Backup data is encrypted while in storage and the encryption keys are accessible in a disaster situation.	False

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

Statement	Statement Name	Status
P1.1.1.7	The organization's approach to Information security risk management is comprehensive; accounting for administrative (people), physical, and technical threats and vulnerabilities.	True
P1.4.1.2	Physical devices and systems within the organization are all inventoried.	True
P1.5.1.3	Physical and logical access controls are integrated and adequately considered in policy.	True
P1.7.15.7	Inherent and residual risk assessments for vendors and third party service providers sufficiently account for administrative, physical, and technical threats and vulnerabilities.	False
P2.3.1.1	Formal physical security policies and procedures exist, are up to date, and include the requirements for physical security and safety planning.	True
P2.3.1.3	Facility physical security risk assessments and security audits are conducted on a regular basis.	False
P2.4.2.1	Utility system design and physical security requirements are documented in policy and supporting procedures.	True
P2.4.2.2	Fire suppression systems are adequate, code-compliant, and protected (within a secure location).	True
P2.4.2.3	Uninterruptible power supplies (UPS) provide sufficient running time.	True
P2.4.2.4	A generator exists, is regularly tested, and has a fuel contract in place.	N/A
P2.4.2.5	Emergency power-off (EPO) switches are near emergency exits in equipment rooms to facilitate rapid power down.	N/A
P2.4.2.6	Emergency switches and valves to cut off water, gas, and other utilities are located near emergency exits and/or equipment rooms.	N/A
P2.4.2.7	The facility is equipped with adequate emergency lighting.	True

P2.4.2.8	Supporting utilities (e.g., electricity, telecommunications, water supply, gas, sewage, ventilation, air conditioning) are alarmed to detect malfunctions.	N/A
P2.4.2.9	All critical utility systems (e.g., electricity, telecommunications, water supply, gas, sewage, ventilation, and air conditioning) are secured.	True
P2.4.2.10	Utility systems and redundancies are tested on a regular basis.	False

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

Statement	Statement Name	Status
P2.4.4.6	Equipment and media disposal practices are sufficiently auditable.	True
P2.4.4.7	Media containing sensitive information is removed from the equipment prior to disposal or re-use.	True
P2.4.4.8	Information is securely overwritten prior to disposal or re-use of equipment	True
P2.4.4.9	Equipment and components that store sensitive information are physically destroyed.	True

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

Statement	Statement Name	Status
P1.1.1.3	The organization's risk management function provides consistent and actionable information for executive management decision-making.	True
P1.1.1.4	Risk decisions (accept, mitigate, avoid, transfer, etc.) are made by executive management personnel with the authority to do so.	True
P1.1.1.5	Risk decisions are identified and prioritized according to defined criteria.	True
P1.10.4.1	Managers actively participate in the development and improvement of the information security program.	True
P1.2.2.4	Policies are consistently reviewed at planned intervals according to a defined schedule.	False
P1.2.2.5	Significant changes within the organization trigger policy reviews and updates.	False
P1.2.2.6	The criteria to be used during information security policy reviews has been formally defined.	True
P1.2.2.7	Information security policies have been formally reviewed within the last twelve months or less.	False
P1.3.3.4	Employees, contractors, and third party resources receive security awareness training on a periodic basis.	False

P1.5.1.8	A periodic review of user accounts and access rights is conducted according to a defined process and procedure.	True
P1.7.10.1	The organization's information security audit requirements are formally documented in policy or procedure.	False
P1.7.10.2	Periodic audits for compliance with information security requirements are performed according to a defined schedule.	False
P1.7.10.3	Access control audits (user accounts, rights, privileges, and other access) are performed on a regular basis.	False
P1.7.11.4	Internal penetration testing is conducted to ensure that controls are operating as intended, and that lateral movement within the organization's networks is sufficiently controlled.	True
P1.7.14.3	New information systems, upgrades and new versions are implemented with formal information security testing.	False
P1.9.2.2	The organization's recovery plans are tested on a periodic basis, and they have been tested within the past twelve (12) months.	False
P1.9.2.3	Recovery plans account for incorporating lessons learned during testing and after an event.	True
P3.8.3.2	There are specific criteria by which the organization measures the effectiveness of its vulnerability management practices.	True
P4.1.3.8	Penetration testing has been conducted against all externally facing systems in the past 12 months.	False

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

Statement	Statement Name	Status
P1.7.10.7	The results of information security audits are shared with senior management.	False
P3.8.3.1	The effectiveness of vulnerability management practices is validated on a periodic basis.	True
P3.8.3.2	There are specific criteria by which the organization measures the effectiveness of its vulnerability management practices.	True

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

Statement	Statement Name	Status
P1.1.2.2	Cyber insurance has been obtained, and selected breach counsel and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.	False
P1.1.2.4	Instructions for how and when to notify insurers is formally documented in an incident response plan.	True

P1.7.15.9	Procedures to handle information security incidents and provide continuation of third party access in the event of an information security incident are defined.	False
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False
P1.9.2.1	The organization's recovery plans are likely to be executed appropriately during and after an event.	False
P1.9.2.2	The organization's recovery plans are tested on a periodic basis, and they have been tested within the past twelve (12) months.	False
P1.9.2.3	Recovery plans account for incorporating lessons learned during testing and after an event.	True
P1.9.2.4	Recovery strategies are updated to reflect the current operating environment.	True
P1.9.2.5	The organization's recovery strategy accounts for public relations.	False
P1.9.2.6	Strategies to address and limit the reputational impact from an event are formally accounted for.	True
P1.9.2.7	The recovery strategy is adequately communicated to all relevant internal personnel and executive management.	True
P3.9.3.1	Backups are taken in accordance with a documented disaster recovery and/or business continuity plan.	False

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

Statement	Statement Name	Status
P1.9.2.2	The organization's recovery plans are tested on a periodic basis, and they have been tested within the past twelve (12) months.	False
P2.3.1.6	Facility evacuation procedures are documented, posted, and tested.	True

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

Statement	Statement Name	Status
P1.10.2.2	A data policy for privacy and protection of personally identifiable information belonging to employees and contractors has been developed and adopted.	True
P1.10.4.3	A formal disciplinary process exists to deal with specific information security non-compliance issues (based on impact or repeat offences).	False

P1.10.4.4	Personnel are rewarded for complying with information security requirements and for exceptional information security performance.	False
P1.10.4.5	Part of an employee's incentives package is related to information security.	True
P1.3.1.1	There is a formal process and procedure for performing background (criminal history, credit, etc.) and verification (prior employment, references, etc.) checks on employees.	True
P1.3.1.2	There is a formal process and procedure to ensure that background (criminal history, credit, etc.) and verification (prior employment, references, etc.) checks on contractors and other third party resources are conducted satisfactorily.	False
P1.3.1.3	Background checks are performed on employees and third parties associates in accordance with their roles, responsibilities, job function, and data sensitivity.	False
P1.3.1.4	The availability of satisfactory character references is considered prior to issuing an offer of employment.	True
P1.3.1.5	Verification of completeness and accuracy of applicant's curriculum vitae is performed prior to issuing an offer of employment.	False
P1.3.1.6	Confirmation of claimed academic and professional qualifications is performed prior to issuing an offer of employment.	False
P1.3.1.7	Background checks are performed in accordance with relevant state and federal laws regarding privacy and protection of information.	True
P1.3.3.3	Employees, contractors, and third party resources receive security awareness training prior to being granted access to information resources.	False
P1.5.2.1	User registration and de-registration practices are carried out in accordance with a documented policy.	True
P1.5.2.6	User de-registration processes adequately ensure that user accounts are disabled or removed immediately after a user leaves the organization.	True

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

Statement	Statement Name	Status
P1.1.1.7	The organization's approach to Information security risk management is comprehensive; accounting for administrative (people), physical, and technical threats and vulnerabilities.	True
P1.3.3.7	Updates to information security policies and practices, and new vulnerabilities and threats are communicated to employees, contractors, and third party resources in a timely manner.	False

P1.7.15.7	Inherent and residual risk assessments for vendors and third party service providers sufficiently account for administrative, physical, and technical threats and vulnerabilities.	False
P3.8.3.1	The effectiveness of vulnerability management practices is validated on a periodic basis.	True
P3.8.3.2	There are specific criteria by which the organization measures the effectiveness of its vulnerability management practices.	True
P3.8.3.3	Vulnerability scanning is conducted regularly, using tools separate from those used to remediate vulnerabilities.	False
P3.8.3.4	Validation processes are authenticated and running with sufficient privileges.	True
P4.1.3.2	External vulnerability scans are conducted on a quarterly basis, or more often.	False
P4.1.3.3	External vulnerability scan reports are reviewed by knowledgeable and authorized personnel.	True
P4.1.3.4	The criteria for conducting external vulnerability scans are documented and repeatable.	False
P4.1.3.5	The criteria for the review of external vulnerability scanning reports are documented and repeatable.	False
P4.1.3.6	Web applications are tested for security on a regular basis.	True
P4.1.3.7	Web applications are tested for security each time a change is made.	N/A
P4.1.3.10	Decision-making criteria and approval for risks and vulnerabilities are documented and followed.	True
P4.4.1.1	There are no critical-severity vulnerabilities (CVSS 10) exposed to the Internet or any other public network.	False
P4.4.1.2	There are no high-severity vulnerabilities (CVSS 7-9) exposed to the Internet or any other public network.	False
P4.4.1.3	There are no known exploitable critical or high-severity vulnerabilities exposed to the Internet or any other public network.	False
P4.4.1.4	There are no medium-severity vulnerabilities (CVSS 4 - 7) exposed to the Internet or any other public network.	False
P4.4.1.5	Medium-severity vulnerabilities were present in less than half of the systems responding to traffic.	False

Maintenance (PR.MA)

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

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

Statement	Statement Name	Status
P1.7.3.5	Instructions for handling errors and other exceptional conditions, which might arise during job execution (including restrictions on the use of system utilities) are documented.	False
P1.7.3.7	Operating procedures are complete and comprehensive to include the proper level of detail (i.e., they include processing and handling, backup, interdependencies with other systems and scheduling requirements, error handling and exceptional conditions, support contacts, system restart and recovery steps, etc.).	False
P1.7.3.8	Documented operating procedures for system activities are treated as formal documents and all changes are authorized by management.	False
P1.7.3.9	Information systems are managed consistently with the same procedures, tools, and utilities for each.	False
P1.7.3.10	Formal operating procedures are protected from unauthorized disclosure, ensuring that access is restricted to personnel who have a business need.	False
P1.7.4.6	Changes are tracked and reviewed; audits of system maintenance activities are being performed.	False
P2.4.4.1	Equipment maintenance security requirements are documented in policy and supported by procedures.	True
P2.4.4.2	Maintenance is performed by personnel who have received specialized training.	True
P2.4.4.3	Records are kept for suspected and actual faults (i.e., system problems).	True
P2.4.4.4	Records are kept of preventive and corrective equipment maintenance activities.	True
P2.4.4.5	Management periodically performs maintenance and tests environmental controls (e.g., fire suppression systems, HVAC controls, power systems) to ensure operational availability.	True
P2.4.4.10	Maintenance personnel have been subjected to background checks.	True

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

Statement	Statement Name	Status
P1.7.15.8	third party contract oversight roles and responsibilities are defined and documented.	False

Protective Technology (PR.PT)

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

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

Statement	Statement Name	Status
P1.5.2.3	All user account management activities are formally authorized and documented to a level that provides an audit trail.	True
P1.7.10.1	The organization's information security audit requirements are formally documented in policy or procedure.	False
P1.7.10.2	Periodic audits for compliance with information security requirements are performed according to a defined schedule.	False
P1.7.10.3	Access control audits (user accounts, rights, privileges, and other access) are performed on a regular basis.	False
P1.7.10.4	All information security audits are coordinated with and through system, application, and/or data owners.	False
P1.7.10.5	The scope, methodology, and timing of all technical audits and testing is agreed to prior to conducting actual audits.	False
P1.7.10.6	All access obtained during audits and testing is monitored and logged to produce a reference trail.	False
P1.7.10.7	The results of information security audits are shared with senior management.	False
P1.7.10.8	Different audit types have been defined (regulatory, internal control, consultative, etc.).	False
P1.7.10.9	Audit results are documented and retained for a period referenced in a retention policy or schedule.	False
P1.7.4.6	Changes are tracked and reviewed; audits of system maintenance activities are being performed.	False
P3.7.3.1	Logs from critical systems are aggregated and correlated to enable the identification of events that span multiple systems.	False
P3.7.3.2	Summary log analysis reports are available and reviewed on a periodic basis.	False
P3.7.4.1	Network time is synchronized with NTP on all devices (e.g., servers, firewalls, switches, workstations).	True
P3.7.4.2	The credentials (username/password) used for day-to-day management of information systems is different than the credentials for managing the organization's logging systems.	False
P3.7.4.3	A separate, isolated logging system is employed to collect and protect log files.	False

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

Statement	Statement Name	Status
P2.4.4.7	Media containing sensitive information is removed from the equipment prior to disposal or re-use.	True

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

No mapping available for this category

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

Statement	Statement Name	Status
P1.7.11.1	Network security, including segregation and/or isolation of critical assets is a documented policy requirement.	False
P1.7.11.3	Data flow diagrams are available for all critical information assets, and they are sufficiently up to date, detailed, and scoped.	False
P1.7.11.4	Internal penetration testing is conducted to ensure that controls are operating as intended, and that lateral movement within the organization's networks is sufficiently controlled.	True
P1.7.11.5	Risk assessments are conducted to determine requirements for the implementation of graduated controls that segregate different logical network domains (e.g., publicly accessible systems, internal networks, and critical assets) and security environments.	True
P1.7.11.6	Mechanisms such as secure gateway, VPN, routing, and switching technologies are implemented sufficiently to enable a graduated set of controls between different logical network domains and to segregate the network by security environments.	True
P1.7.11.7	Segregation of networks is based on the value and classification of information stored and/or processed in the network, levels of trust, lines of business, or need-to-know.	True
P1.7.11.8	Gateway devices are configured to filter traffic between domains and block unauthorized access in accordance with the organization's access control policy.	True
P3.1.2.1	Firewalls (or other packet filtering and control devices) are used to secure traffic between networks at remote sites.	N/A
P3.1.2.2	Systems at remote sites are unable to access untrusted networks (e.g., the Internet) without passing through firewalls (or other packet filtering and control devices).	N/A
P3.1.2.3	Egress and ingress traffic restrictions are in place and are	N/A

	limiting traffic to only what is required for operational purposes between WAN segments.	
P3.1.2.4	Traffic between sites is adequately protected from eavesdropping.	N/A
P3.1.3.1	Switch ports are only active when necessary and approved; otherwise, the ports are disabled or secured using other means.	True
P3.1.3.2	The organization leverages port-based network access control (802.1x).	False
P3.1.3.3	Network segmentation is adequately leveraged to isolate and protect networked systems.	True
P3.1.3.4	The organization has implemented a separate, isolated management network.	True
P3.1.3.5	Network devices are managed using secure protocols only.	True
P3.1.3.6	Unmanaged network equipment (switches and hubs) is not employed for network connectivity; all network equipment is managed.	True
P3.1.3.8	Security-specific systems are deployed on a dedicated network subnet.	True

Subcategory: PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

Statement	Statement Name	Status
P2.4.2.3	Uninterruptible power supplies (UPS) provide sufficient running time.	True
P2.4.2.4	A generator exists, is regularly tested, and has a fuel contract in place.	N/A
P2.4.2.10	Utility systems and redundancies are tested on a regular basis.	False
P3.1.2.6	Critical business operations at secondary sites are supported by multiple redundant connections to the main site.	N/A
P3.1.3.7	Critical systems are equipped with redundant network connections.	True
P3.1.3.9	Network device management processes are redundant and resilient.	True
P3.4.3.2	The storage environment is supported by an appropriate level of redundancy (e.g., local, SAN, NFS, iSCSI).	True
P3.9.3.2	Resilience requirements are documented and implemented in accordance with a business impact analysis.	False

DETECT Function

Anomalies and Events	Security Continuous	Detection Processes
569	616	533

NIST CSF DETECT Function includes the following Categories:

- **Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Anomalies and Events (DE.AE)

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

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

Statement	Statement Name	Status
P1.7.11.3	Data flow diagrams are available for all critical information assets, and they are sufficiently up to date, detailed, and scoped.	False

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

Statement	Statement Name	Status
P3.4.3.1	The organization regularly scans storage systems in search of unusual or unauthorized file storage.	True
P3.7.3.2	Summary log analysis reports are available and reviewed on a periodic basis.	False

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

Statement	Statement Name	Status
P3.7.3.1	Logs from critical systems are aggregated and correlated to enable the identification of events that span multiple systems.	False
P3.7.3.2	Summary log analysis reports are available and reviewed on a periodic basis.	False

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

Statement	Statement Name	Status
P1.7.4.3	The organization's change management processes include all necessary elements (identifying and recording changes, planning, and testing changes, assessment of potential impacts including security impacts, formal approval procedure, communication of change details, back-out plan, etc.).	True
P1.9.2.6	Strategies to address and limit the reputational impact from an event are formally accounted for.	True

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

Statement	Statement Name	Status
P1.1.1.2	Organizational risk tolerance is determined and clearly expressed (e.g., an acceptable risk score and/or risk threshold has been established, and defined criteria for which risks/risk levels require specific actions have been agreed upon).	False

Security Continuous Monitoring (DE.CM)

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

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

Statement	Statement Name	Status
P1.10.5.7	Financial accounts are monitored and balanced daily.	True
P3.2.1.5	The organization consistently monitors remote access connection attempts and traffic.	False

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

Statement	Statement Name	Status
P2.3.1.9	Security guards are employed and are formally trained and tested on all facility security and emergency response procedures.	N/A
P2.3.4.5	A manned reception area or other means to control physical access to the site or building is in place.	True
P2.3.4.8	Public spaces are covered by camera surveillance.	False
P2.3.4.9	Activities occurring within public spaces are actively monitored.	True
P2.3.5.8	Employees, contractors, and external parties have been instructed to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.	True
P2.3.5.10	All exits have a card-in/card-out audit trail or security cameras cover all exits.	True
P2.3.7.5	Public, delivery, and loading areas are staffed.	True
P2.3.7.6	Public, delivery, and loading areas are covered by surveillance cameras (CCTV).	False
P2.4.2.8	Supporting utilities (e.g., electricity, telecommunications, water supply, gas, sewage, ventilation, air conditioning) are alarmed to detect malfunctions.	N/A

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

Statement	Statement Name	Status
P1.10.4.2	Managers regularly review the level of compliance with information security policies and procedures within their respective areas of responsibility.	False
P1.10.4.4	Personnel are rewarded for complying with information	False

	security requirements and for exceptional information security performance.	
P1.10.4.5	Part of an employee's incentives package is related to information security.	True
P1.3.3.8	The effectiveness of information security training and awareness exercises is measured in a quantifiable manner.	False

Subcategory: DE.CM-4: Malicious code is detected

Statement	Statement Name	Status
P3.6.1.6	Mobile devices employ anti-malware protection.	False

Subcategory: DE.CM-5: Unauthorized mobile code is detected

Statement	Statement Name	Status
P3.6.1.6	Mobile devices employ anti-malware protection.	False

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

Statement	Statement Name	Status
P1.1.1.6	Threats, both internal and external, are identified and documented as part of the risk management practice.	True
P1.7.15.1	Formal policies and procedures to identify, evaluate, and manage risks associated with utilizing third party providers exist.	True
P1.7.15.8	third party contract oversight roles and responsibilities are defined and documented.	False
P2.4.4.4	Records are kept of preventive and corrective equipment maintenance activities.	True
P2.4.4.6	Equipment and media disposal practices are sufficiently auditable.	True

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

Statement	Statement Name	Status
P1.4.1.2	Physical devices and systems within the organization are all inventoried.	True
P1.4.1.3	Software platforms and applications within the organization are inventoried.	False
P1.4.1.5	All physical, software, and data assets are formally accounted for throughout the organization.	False

P1.4.1.8	Formal asset reconciliation processes are sufficient to account for lost, damaged, and stolen assets.	False
P3.1.3.1	Switch ports are only active when necessary and approved; otherwise, the ports are disabled or secured using other means.	True
P3.1.3.2	The organization leverages port-based network access control (802.1x).	False
P3.2.1.5	The organization consistently monitors remote access connection attempts and traffic.	False
P4.1.3.1	Periodic scans for back-channel connections (those that bypass the DMZ) are conducted.	False
P4.3.1.1	The organization regularly audits the ports that are open to the Internet.	False

Subcategory: DE.CM-8: Vulnerability scans are performed

Statement	Statement Name	Status
P3.8.3.1	The effectiveness of vulnerability management practices is validated on a periodic basis.	True
P3.8.3.2	There are specific criteria by which the organization measures the effectiveness of its vulnerability management practices.	True
P3.8.3.3	Vulnerability scanning is conducted regularly, using tools separate from those used to remediate vulnerabilities.	False
P3.8.3.4	Validation processes are authenticated and running with sufficient privileges.	True
P4.1.3.1	Periodic scans for back-channel connections (those that bypass the DMZ) are conducted.	False
P4.1.3.2	External vulnerability scans are conducted on a quarterly basis, or more often.	False
P4.1.3.3	External vulnerability scan reports are reviewed by knowledgeable and authorized personnel.	True
P4.1.3.4	The criteria for conducting external vulnerability scans are documented and repeatable.	False
P4.1.3.5	The criteria for the review of external vulnerability scanning reports are documented and repeatable.	False

Detection Processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

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

No mapping available for this category

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

Statement	Statement Name	Status
P1.10.1.2	Legal and regulatory requirements regarding information security, including privacy and civil liberties obligation, are well-understood and managed.	True
P1.10.2.1	A data policy for privacy and protection of personally identifiable information belonging to customers has been developed and adopted.	True
P1.10.2.2	A data policy for privacy and protection of personally identifiable information belonging to employees and contractors has been developed and adopted.	True
P1.10.2.3	The organization's privacy requirements have been formally communicated to all personnel involved in the processing of personally identifiable information.	True
P1.10.2.4	The organization's privacy policy accounts for all relevant regulations and legislation, especially when dealing with data belonging individuals living in other countries.	True
P1.3.1.7	Background checks are performed in accordance with relevant state and federal laws regarding privacy and protection of information.	True
P1.7.10.2	Periodic audits for compliance with information security requirements are performed according to a defined schedule.	False

Subcategory: DE.DP-3: Detection processes are tested

Statement	Statement Name	Status
P1.7.11.4	Internal penetration testing is conducted to ensure that controls are operating as intended, and that lateral movement within the organization's networks is sufficiently controlled.	True
P1.7.14.3	New information systems, upgrades and new versions are implemented with formal information security testing.	False
P1.9.2.2	The organization's recovery plans are tested on a periodic	False

	basis, and they have been tested within the past twelve (12) months.	
P2.3.1.9	Security guards are employed and are formally trained and tested on all facility security and emergency response procedures.	N/A
P4.1.3.6	Web applications are tested for security on a regular basis.	True
P4.1.3.7	Web applications are tested for security each time a change is made.	N/A
P4.1.3.8	Penetration testing has been conducted against all externally facing systems in the past 12 months.	False

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

Statement	Statement Name	Status
P1.3.3.7	Updates to information security policies and practices, and new vulnerabilities and threats are communicated to employees, contractors, and third party resources in a timely manner.	False
P1.7.3.6	In the event of unexpected operational or technical difficulties, support, and escalation contacts (including external support contacts) are documented.	True

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

Statement	Statement Name	Status
P1.10.4.1	Managers actively participate in the development and improvement of the information security program.	True
P1.9.2.3	Recovery plans account for incorporating lessons learned during testing and after an event.	True

RESPOND Function

Response Planning	Communications	Analysis
693	603	565
Mitigation	**Improvements**	
721	300	

NIST CSF RESPOND Function includes the following Categories:

- **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- **Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.
- **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Response Planning (RS.RP)

Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

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

Statement	Statement Name	Status
P1.1.2.4	Instructions for how and when to notify insurers is formally documented in an incident response plan.	True
P1.6.1.9	The loss of cryptographic keys or other compromise of encryption is accounted for in the organization's incident response processes.	False
P1.7.15.9	Procedures to handle information security incidents and provide continuation of third party access in the event of an information security incident are defined.	False
P2.3.1.4	A comprehensive, and up to date security plan and/or emergency response plan exists for the facility.	True

Communications (RS.CO)

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

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

Statement	Statement Name	Status
P1.1.2.2	Cyber insurance has been obtained, and selected breach counsel and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.	False
P1.3.3.6	The organization's information security awareness program includes key elements such as management's commitment to information security, complying with security requirements, legal responsibilities, basic security procedures, and key contact points (for incident reporting and additional information).	True
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False

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

Statement	Statement Name	Status
P1.3.3.6	The organization's information security awareness program includes key elements such as management's commitment to information security, complying with security requirements, legal responsibilities, basic security procedures, and key contact points (for incident reporting and additional information).	True
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False
P2.3.5.8	Employees, contractors, and external parties have been instructed to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.	True
P2.3.7.10	Incoming and outgoing activities occur in separate physical areas.	False

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

Statement	Statement Name	Status
P1.1.2.4	Instructions for how and when to notify insurers is formally documented in an incident response plan.	True
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False

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

Statement	Statement Name	Status
P1.1.2.2	Cyber insurance has been obtained, and selected breach counsel and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.	False
P1.1.2.4	Instructions for how and when to notify insurers is formally documented in an incident response plan.	True

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

No mapping available for this category

Analysis (RS.AN)

Analysis is conducted to ensure adequate response and support recovery activities.

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

No mapping available for this category

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

Statement	Statement Name	Status
P1.10.4.3	A formal disciplinary process exists to deal with specific information security non-compliance issues (based on impact or repeat offences).	False

Subcategory: RS.AN-3: Forensics are performed

Statement	Statement Name	Status
P1.1.2.2	Cyber insurance has been obtained, and selected breach counsel and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.	False

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

No mapping available for this category

Subcategory: RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

Statement	Statement Name	Status
P1.7.15.10	Contracts with vendors and third party service providers contain necessary security provisions such as prevention requirements, incident reporting requirements and/or the organization's right to audit.	False
P2.3.5.8	Employees, contractors, and external parties have been instructed to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.	True
P4.2.1.1	The organization performs searches of the Internet on a regular basis, looking for sensitive information that may have	False

	been exposed.	
P4.2.1.2	The organization performs searches of common social media sites on a regular basis, looking for sensitive information that may have been exposed.	False
P4.2.1.3	The organization performs searches of common file sharing sites on a regular basis, looking for sensitive information that may have been exposed.	False
P4.2.1.4	Sensitive information was not discovered in publicly accessible locations on one or more of the organization's Internet-accessible systems.	False
P4.2.1.5	No other publicly available information was discovered about the organization that could be valuable to an attacker.	True

Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Subcategory: RS.MI-1: Incidents are contained

Statement	Statement Name	Status
P1.1.2.2	Cyber insurance has been obtained, and selected breach counsel and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.	False
P1.1.2.4	Instructions for how and when to notify insurers is formally documented in an incident response plan.	True

Subcategory: RS.MI-2: Incidents are mitigated

Statement	Statement Name	Status
P1.1.1.4	Risk decisions (accept, mitigate, avoid, transfer, etc.) are made by executive management personnel with the authority to do so.	True
P1.1.2.2	Cyber insurance has been obtained, and selected breach counsel and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.	False
P1.1.2.4	Instructions for how and when to notify insurers is formally documented in an incident response plan.	True

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

Statement	Statement Name	Status
P1.1.1.4	Risk decisions (accept, mitigate, avoid, transfer, etc.) are made by executive management personnel with the authority to do so.	True
P3.8.3.2	There are specific criteria by which the organization measures the effectiveness of its vulnerability management practices.	True
P4.1.3.3	External vulnerability scan reports are reviewed by knowledgeable and authorized personnel.	True
P4.1.3.4	The criteria for conducting external vulnerability scans are documented and repeatable.	False
P4.1.3.5	The criteria for the review of external vulnerability scanning reports are documented and repeatable.	False
P4.1.3.10	Decision-making criteria and approval for risks and vulnerabilities are documented and followed.	True

Improvements (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

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

No mapping available for this category

Subcategory: RS.IM-2: Response strategies are updated

No mapping available for this category

RECOVER Function

Recovery Planning	Improvements	Communications
609	667	621

NIST CSF RECOVER Function includes the following Categories:

- **Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.
- **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Recovery Planning (RC.RP)

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

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

Statement	Statement Name	Status
P1.9.2.1	The organization's recovery plans are likely to be executed appropriately during and after an event.	False
P1.9.2.5	The organization's recovery strategy accounts for public relations.	False
P1.9.2.6	Strategies to address and limit the reputational impact from an event are formally accounted for.	True
P1.9.2.7	The recovery strategy is adequately communicated to all relevant internal personnel and executive management.	True

Improvements (RC.IM)

Recovery planning and processes are improved by incorporating lessons learned into future activities.

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

Statement	Statement Name	Status
P1.9.2.2	The organization's recovery plans are tested on a periodic basis, and they have been tested within the past twelve (12) months.	False
P1.9.2.3	Recovery plans account for incorporating lessons learned during testing and after an event.	True

Subcategory: RC.IM-2: Recovery strategies are updated

Statement	Statement Name	Status
P1.9.2.2	The organization's recovery plans are tested on a periodic basis, and they have been tested within the past twelve (12) months.	False
P1.9.2.4	Recovery strategies are updated to reflect the current operating environment.	True
P1.9.2.7	The recovery strategy is adequately communicated to all relevant internal personnel and executive management.	True

Communications (RC.CO)

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Subcategory: RC.CO-1: Public relations are managed

Statement	Statement Name	Status
P1.1.2.2	Cyber insurance has been obtained, and selected breach counsel and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.	False
P1.9.2.5	The organization's recovery strategy accounts for public relations.	False

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

Statement	Statement Name	Status
P1.1.2.2	Cyber insurance has been obtained, and selected breach counsel and vendors (forensics firm, public relations firm, crisis management firm, etc.) are included in the organization's incident response plan.	False
P1.9.2.6	Strategies to address and limit the reputational impact from an event are formally accounted for.	True

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

Statement	Statement Name	Status
P1.3.3.6	The organization's information security awareness program includes key elements such as management's commitment to information security, complying with security requirements, legal responsibilities, basic security procedures, and key contact points (for incident reporting and additional information).	True
P1.9.2.7	The recovery strategy is adequately communicated to all relevant internal personnel and executive management.	True

You have reached the end of the report.

Please contact Fossa University with any questions or concerns about the content of this report.