MCS
Cloud • Security • Software • Services

Information Security Program Risk Assessment Report

ACME CORPORATION

Contacts

DEG Contacts			
Name	**Email**	**Phone**	**Project Role**
Patrick Tyer	patrick.tyer@digitaleragroup.com	(321) 332-5362	Strategic Consultant
Carlos Rodriguez	carlos.rodriguez@digitaleragroup.com	(843) 473-8226	Strategic Consultant

Acme Inc. Contacts			
Name	**Email**	**Phone**	**Project Role**
Road Runner	rr@looneytunes.com	(212) 555-1212	Vice President, Information Technology

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission.

DigitalEra Group (DEG) treats the contents of a security assessment as company confidential material and will not disclose the contents of this document to anyone without written permission.

Table of Contents

Introduction

Greater volumes of confidential information are being stored and transmitted on computer networks each day, which makes them more inviting as targets of attacks and misappropriate use of information and assets. At the same time, there is a growing computer literacy among users of computers resulting in far greater numbers of people having the skills to misappropriate or corrupt sensitive information stored on network servers. The potential for attacks on Acme Inc.'s servers, web, and mobile applications is exacerbated, as the organization becomes more Internet enabled.

Security threats range from inquisitive insiders or outsiders and to well-organized, technically aware intruders that could gain access to Acme Inc.'s information or deny access to the systems. Much like the Internet itself, the volume and sophistication of these threats grow each year. Aimed at measuring the security posture of Acme Inc.'s environment and to identify areas of improvement, DigitalEra Group completed a Security Risk Assessment of the Information Security Program with a focus on the following core components:

- Access Control
- Identity & Access Management
- Account Management
- Configuration Management
- Monitoring and Malware
- Remote Access Control
- Asset Management
- Information Security Incident Management
- Business Continuity Management
- Portable/Mobile/Wireless
- Risk Management & Assessment

Methodology and Approach

DigitalEra Group uses a multi-part methodology that leverages our expertise in the industry as well as a common guideline framework to provide a consistent and comprehensive analysis of the Client's Information Security Program. Our assessment utilized a blend of best practices control standards and frameworks tailored to Acme Inc.'s industry and structure. Particularly, the National Institute of Science and Technology (NIST) Cybersecurity Framework (CSF) set of security controls were used as an assessment focal point. The report is divided into four parts:

1. An Executive Dashboard meant to provide a quick high-level summary to the board and top executives.
2. A Priority Roadmap, with detailed recommendations for improvement, both strategic and tactical, laid out in a tabular form, prioritized based on Acme Inc.'s current threat landscape and internal capabilities. The Roadmap captures the current state (area of improvement), the Risk, future state (recommendation), and Residual Risk.

3. A detailed list of questions asked and answers collected during the 3-day assessment engagement.
4. A Guidance section, providing detailed guidance on best practice process to assist in developing those areas of improvement.

Standard Framework

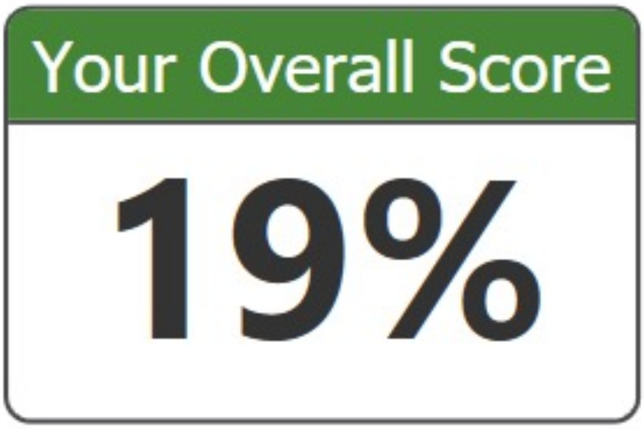
The methodology used includes the use of the NIST Cybersecurity Framework (CSF) as a starting point that provides a series of requirements based on the tailoring of controls for this sector. Lastly, we pull together our industry expertise and knowledge to expand the detail within each requirement and add new requirements as a part of the assessment.

Detailed Analysis

As the analysis begins, DigitalEra Group requests several key documents in association with the framework listed above as well as key documents that must be in place to successfully carry out an Information Security program. These may include diagrams, policies, procedures, and other key material. During the document gathering and review process, DigitalEra Group will make inquiries of a series of interview questions with key stakeholders of the Information Security program as well as those in specific functional and technology areas. The purpose of these inquiries is to identify aspects of the program that may not be documented as well as to obtain a solid understanding of the documentation itself.

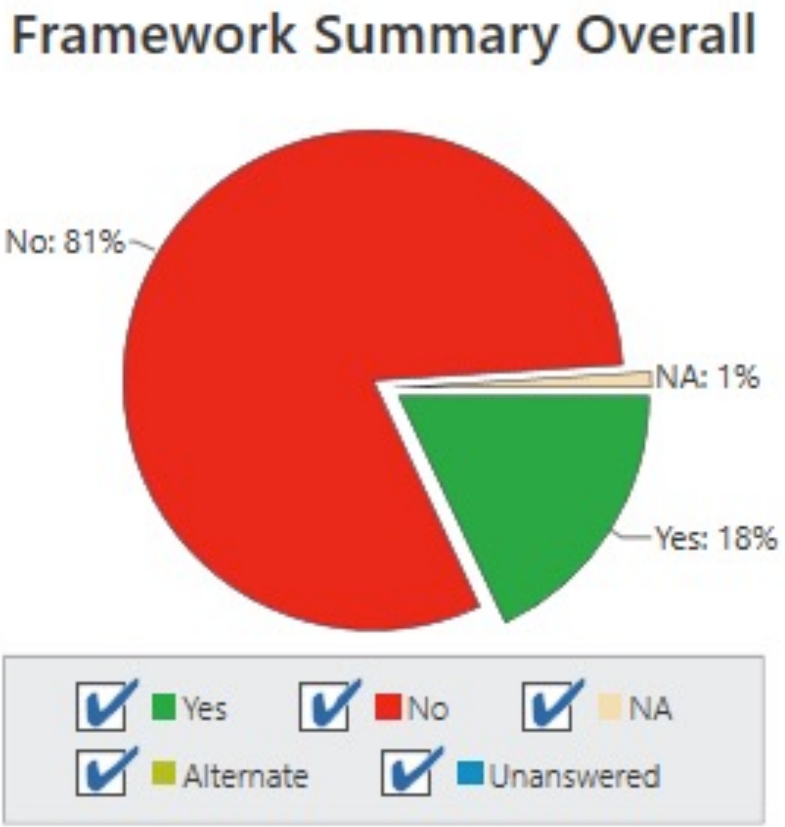
Executive Summary Dashboard

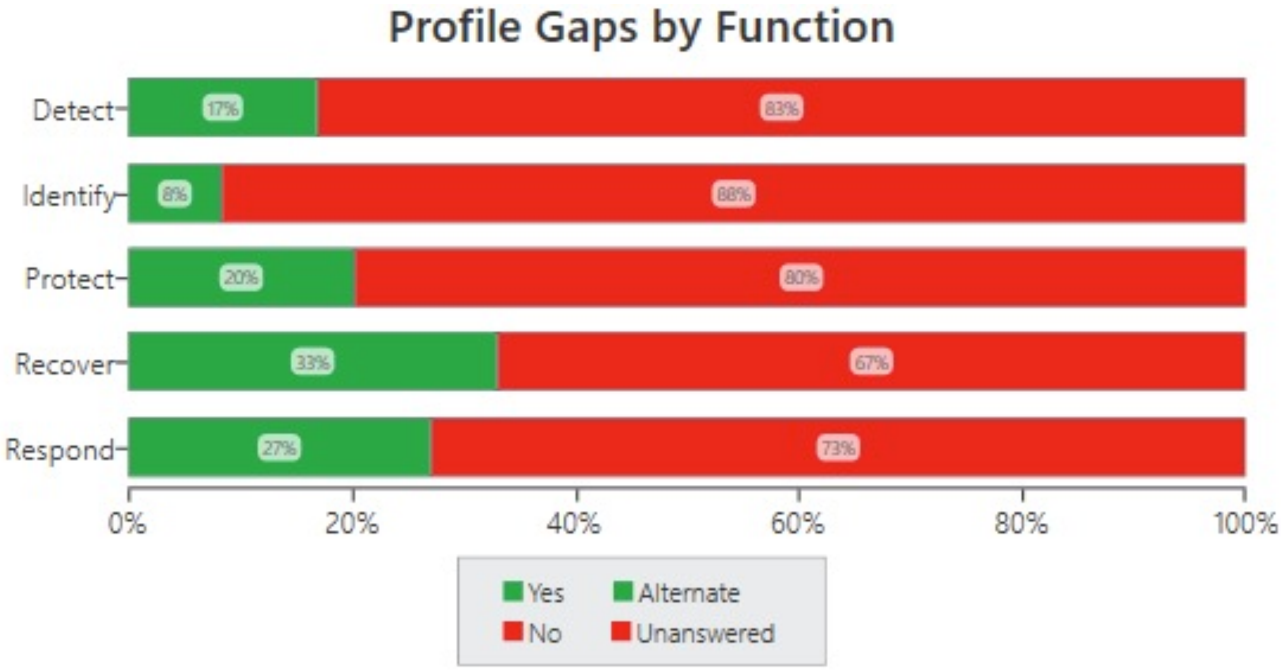
DEG noted a lack of enforcement of some of the existing policies and their support procedures, as well as several instances of missing Information Security Program key components or ineffective existing controls or technologies. Several key security controls were also not being implemented within Acme Inc.'s environment. The following matrix is a summary of the assessment's overall results, Information Security key process effectiveness, their technology maturity and capability, and existing level of investment.



Your Overall Score

19%


Framework Summary Overall
No: 81%
NA: 1%
Yes: 18%
☑ 🟩 Yes
☑ 🟥 No
☑ NA
☑ Alternate
☑ Unanswered


Profile Gaps by Function
Detect
17%
83%
Identify
8%
88%
Protect
20%
80%
Recover
33%
67%
Respond
27%
73%
0%
20%
40%
60%
80%
100%
🟩 Yes
🟩 Alternate
🟥 No
🟥 Unanswered

Process	Overall Effectiveness
Access Control	🔴
Identity & Access Management	🟡
Account Management	🟡
Configuration Management	🔴
Monitoring and Malware	🟡
Remote Access Control	🔴
Asset Management	🟡
Information Security Incident Management	🟡
Business Continuity Management	🔴
Portable/Mobile/Wireless	🔴
Risk Management & Assessment	🔴

Legend:

🟢	Control area is overall adequate, from an effectiveness or efficiency perspective; technology solutions actual capabilities address needs.
🟡	Efficiency or effectiveness opportunities for improvement were noted; technology solutions actual capabilities address some, but not all needs.
🔴	Inefficiency or ineffectiveness noted; (People, Process, and Technology): technology solutions actual capabilities do not address needs, or process may not be formalized, or people may not be

The following is a summary of high-level risk/priority items found during our assessment. These items are the root causes of our ratings in the matrix above. All High Risk items should be remediated first, as they pose the greatest risk to the organization, and will yield maximum return on investment.

High	The absence of ratification of an updated and comprehensive set of policies is a key factor hindering the overall effectiveness of the Information Security Program.
Med	The absence of a formalized and approved Information Security Strategic Plan aligned with Acme Inc.'s business objectives, leads to a reactive and somewhat unorganized approach to information security.
High	The absence of two-factor authentication for remote users and administrators for both corporate systems and applications (products) may lead to security breaches, digital crime and Internet fraud.
Med	An Asset Management solution is in place. However, the solution does not currently track all mobile endpoints. Rogue Assets or access points may be introduced creating unmanaged or insecure end points.
High	The absence of a formalized Configuration Management Framework prevents IT from consistently applying standardized agreed upon best practice security and hardening standards to the organization's assets including servers, databases, network appliances, bring your own device (BYOD), and workstations.
Med	The absence of detailed control requirements of a Security Information and Events Management (SIEM) solution, combined with absence of dedicated personnel to manage and report on the Monitoring function, hinders the use of existing SIEM technologies. It may lead to failure to discover intrusions or breaches, as well as failure to discover system performance degradation, and overload incidents.
High	The absence of a comprehensive formalized Incident Handling & Crisis Management Program and its support processes may lead to the organization failing to detect, contain, eradicate and recover from a security incident in a timely manner.
High	The absence of a Threat and Vulnerability Management Program may lead to vulnerable systems and products leading to potential security breaches, digital crime and Internet fraud.
Low	The absence of a formal and dedicated Privacy Program may result in a breach of customer personally identifiable information, leading to potential legal liability and compliance issues.
Med	The absence of testing the Disaster Recovery plan, and the disaster recovery site, may lead failure of recovery efforts in the case of an actual disaster.

Priority Roadmap

The following roadmap provides a prioritized approach and details the domains reviewed, their current state observations, current risk, their future state recommendations, residual risk, and action plan.

Domain	Current State	Risk	Future State	Residual Risk
Ri sk M an		🟥		Low

	There is no formalized process in place to continuously identify, define, and formally document relevant statutory, regulatory, and contractual requirements for each system/product type, including those for the protection of customer information and the legal and ethical responsibilities to protect this information.	High	A comprehensive Information Risk Management Framework (RMF) shall be developed and formalized, with assigned roles and responsibilities to continuously identify and address Risk to the Organization, including 3rd party risk, compliance risk, and information security risk. The organization shall utilize an authoritative framework standard such as NIST Special Publication 800-37 R2 Risk Management Framework for Information Systems and Organizations 2.0	NIST SP 800-53 (PM, PS, RA)
	There is no formalized control framework to address risk profiles of systems/products including relevant statutory, regulatory, and contractual requirements.			
	There is no formalized Risk Management framework in place to continuously identify risk to the organization, formally rate, rank, and prioritize risk, track this risk, provide recommendations on remediating such risk, and report to stake holders on the state of the risk in the group.			
	There is no electronic records retention process detailing records management and protection from loss, disclosure, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	Med	Guidelines shall be issued by the organization on the ownership, classification, retention, storage, handling and disposal of all records and information. Designated senior management within the organization shall review and approve the security categorizations and associated guidelines.	

		🟧	All regulatory and legislative retention requirements shall be met.	

Domain	Current State	Risk	Future State	Residual Risk
Privacy	Currently there is no privacy program or policies to ensure individuals’ right to adequate notice of the uses and disclosures of personally identifiable information that may be made by the organization, and of the individual's rights and the entity's legal duties.	High	The Information Security Officer shall document missing policies and procedures and submit to the Board for approval. All new policies and procedures shall be enforced, and incorporated in the annual information security training.	Low NIST SP 800-53 (Appendix J)

Domain	Current State	Risk	Future State	Residual Risk
Asset Man		🟧		Low

	Asset management solution does not currently keep track of remote mobile endpoints.	Med	The organization shall identify and inventory all assets and services including information (e.g. PII), encrypted or unencrypted, wherever it is created, received, maintained or transmitted, including organizational and third-party sites, and document the importance of these assets. Locations in which PII constitutes a designated record set shall be explicitly identified in the asset inventory. Approved bring your own device (BYOD) equipment shall also be included on the organization's inventories if connecting to its systems or storing business information. The asset inventories shall also include all information necessary to recover from a disaster, including type or classification of the asset, format, location, backup information, license information, and the importance of these assets (business value). The inventory shall not duplicate other inventories unnecessarily, but it shall be ensured that the content is aligned. The organization shall maintain an inventory of authorized wireless access points, including a documented business justification, to support unauthorized WAP identification.	NIST SP 800-53 (CM, PM, AC, CA, PL, CP, RA, SA, SC)

Domain	Current State	Risk	Future State	Residual Risk
Information Security Incident Management	Currently, the incident handling and crisis management plan is not board approved and is not enforced, to ensure timely and proper reaction to an incident or a crisis. Further, the plan lacks key elements of an effective incident handling and crisis management plan. The existing SIEM is not monitoring servers, or ingesting log or event data from all organizational data sources. The existing SIEM is not manned. The existing SIEM is not configured to alert responsible stakeholders when there is a critical security or performance event.	Med	Formal information security event reporting procedures to support the corporate direction (policy) shall be established, together with an incident response program, setting out the formal governance structure, tactical actions to be taken on receipt of a report of an information security event, treating the breach as discovered, and the timeliness of reporting and response. Incident playbooks shall be developed for handling specific types of common incidents. Organization-wide standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be	Low

Domain	Current State	Risk	Future State	Residual Risk
Policies & Procedures	The following policies and their support procedures have not been documented and formalized: Sensitive System Isolation Risk Management Configuration Management Capacity Management Protection Against Malicious and Mobile Code Media Handling & Protection Procedures Monitoring & Logging Network & Perimeter Security Secure Log On Privacy	🟥 High	The Information Security Officer shall document missing policies and procedures and submit to the Board for approval. All new policies and procedures shall be enforced, and incorporated in the annual information security training.	Low NIST SP 800-53 (CA, PM, PS, PL)
		🟧	included in the incident notification.	NIST SP 800-53 (CA, CP, IR)

Primary Recommendations

After considering the preceding analysis of the organization’s current information security posture, the following recommendations and corresponding justifications are presented.

Recommendation	Justification
Use a secure gateway when using RDP across the environment	A much safer alternative is to close RDP access from outside the network, and make it accessible only from a secure protocol, such as SSL VPN on your firewall, or Microsoft's own Remote Desktop Gateway service.
Implement a Password Management solution	A password manager assists in generating and retrieving complex passwords, and potentially storing such passwords in an encrypted database or calculating them on demand.
Expand use of Okta	Okta is already present in the environment. Recommend using this Access Management solution in its full capability to implement a robust Single Sign-On (SSO) solution across the organization.
Include mobile endpoints in your Asset Management Plan	Laptops out in the field need to be tracked in order to have full visibility of your organizational assets.
Documents and update network flow diagrams and firewall rules	The organization needs to carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Establishing, developing, documenting, and maintaining under configuration control, a baseline system and network configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture.
Perform an RPO/RTO analysis	Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities such as attack surface reduction and tailored acquisition strategies.

Regular testing of backup generators	Regular testing, maintenance, exercising, and inspection can help keep standby generators ready to perform when needed.
Establish a comprehensive security training program	Determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content should include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents, including addressing awareness of the need for operations security.
Establish a Vulnerability Management Program	Continuous security assessments ensure that information security is built into organizational information systems, identify weaknesses and deficiencies early in the development process, provide essential information needed to make risk-based decisions as part of security authorization processes, and ensure compliance to vulnerability mitigation procedures. Vulnerability scanning and system monitoring assist in maintaining the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail, as deemed necessary by the organization, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.
Consider implementing a Mobile Device Management (MDM) solution	Given the amount of mobile devices within the organization’s purview, a MDM solution can be leveraged to secure, monitor, manage, and support mobile

	devices belonging to the company or the employees themselves.
Establish an Incident Response (IR) Plan and consider the use of an IR retainer	An IR Plan provides the organization with a roadmap for implementing its incident response capability and describes the structure and organization of the incident response capability. Implementing cyber security defenses such as creating incident response plans and having an IR retainer is far more cost effective than waiting for disaster to strike and dealing with the fallout.
Implement a solution for data-at-rest-encryption	Data-at-rest encryption helps to ensure that data is secure right down to the storage medium in which it is held in a number of ways. Hardware-level encryption, firmware protection for the hard drive, and instant, secure erasing technology allow devices to be retired with minimal risk of data misuse.
Use static and dynamic application testing (SAST and DAST) during application development sprints	Application Security solutions – the combination of people, process and technology – must address the entire product lifecycle. They must provide visibility and control across the entire SDLC. SAST and DAST are complementary application security testing tools that should be used in combination. Organizations should pay attention to finding and fixing serious flaws during development.

Assessment Questions and Results

The following section lists the answers given to the NIST CSF set of questions posed during the assessment and constitute the current implementation status.

Asset Management 1		
Question:	Physical devices and systems within the organization are inventoried	Yes

Comment:	Presently, asset management is being tracked by multiple spreadsheets. PDQ is also used, as well as AD. Will eventually move to Ultimate HR system and Sharepoint. Mobile phones are tracked by a spreadsheet and by an AT&T poral. Laptopts are inventoried with a SharePoint list.

Asset Management 2		
Question:	Software platforms and applications within the organization are inventoried	No
Comment:	Software is being tracked via PDQ. However, PDQ has no visibility to external mobile endpoints. Recommend tracking software for laptops.	

Asset Management 3		
Question:	Organizational communication and data flows are mapped	No
Comment:	Network diagrams and architectures need to be updated. All data flow paths within the organization are not clearly monitored. Recommend regular updates to network diagrams, network flow diagrams and implemented firewall rules.	

Asset Management 4		
Question:	External information systems are catalogued	No
Comment:	SOPHOS, Meraki switches, O365, Ultimate SaaS products, SalesForce, Monday.com, The following are not actively catalogued: Mimecast, Iland (DR), GRID Suite (web servers, Enterprise, GRIDWeb, mass communications, DrawBridge Mobile), JenARC, JobVite, Zoom, ZenDesk, ZenDesk Talk, SharePoint, Association Voice, Expensify, GoToAssist. External systems (e.g., laptops for RDs and Project Managers) are not fully catalogued. BCP needs to be updated to include all external vendors and critical software/application dependencies.	

Asset Management 5		
Question:	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	No
Comment:	Formal data and asset classification needs to be completed. An RPO/RTO assessment needs to be conducted to determine the criticality of each system as well as the data classification for each system.	

Asset Management 6		
Question:	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	No
Comment:	A Contingency Plan is not in place. A Disaster Recovery Plan exists but only currently covers hurricane threats. Needs to be expaned to cover Cybersecurity. C-CERT (Acme Inc. Computer Emergency Response Team) has been created. Formal Cybersecurity roles have not been designated for the organization.	

Business Environment 1		
Question:	The organization's role in the supply chain is identified and communicated	N/A
Comment:	No clear documentation on supply chain as the company model is more consulting.	

Business Environment 2		
Question:	The organization's place in critical infrastructure and its industry sector is identified and communicated	No
Comment:	Recommend performing a new RPO/RTO exercise to identify key infrastructure pieces and establish recovery timelines and criticalities. BCP identifies key infrastructure pieces. However, there is not testing procedures in place.	

Business Environment 3		
Question:	Priorities for organizational mission, objectives, and activities are established and communicated	No
Comment:	Performing a new RPO/RTO exercise to identify key infrastructure pieces and establish recovery timelines and criticalities. Recommend exercise to determine key assets which affect PII and the confidentiality, integrity and availability (CIA) of data.	

Business Environment 4		
Question:	Dependencies and critical functions for delivery of critical services are established	No
Comment:	Failover is tested on a quarterly basis for Iland hotsite backups. Failover is for functionality testing only and does not test for data integrity. No application testing is performed. Critical services are identified and listed on a central, physical copy (BCP). Backup generator for building will run for ~3 days and is tested weekly. Contract is in place with fuel vendor. Prioritization unknown. Server Battery backup will run for approximately 30 minutes and is not tested regularly. APCs on workstations have a run time of 15 minutes. These are not tested regularly. Telecommunications providers - Windstream is the telecommunications provider. Comcast provides separate access for WiFi and cameras. Recommend regular testing of backup generators and UPSs. Recommend	

	redundant network connectivity for production environment.

Business Environment 5		
Question:	Resilience requirements to support delivery of critical services are established	No
Comment:	The organzation's contingency plan does not tie into recovery objectives and timelines. A redundant site is in place with Iland. Capacity planning is in place as the environment can grow as needed. A contract is in place with Iland to provide failover services.	

Governance 1		
Question:	Organizational information security policy is established	No
Comment:	With regards to IT Security policies, the users are briefed on acceptable use and password requirements during employee on-boarding. No other IT Security policies are in place. Recommend establishing a more robust training program along with annual training requirements.	

Governance 2		
Question:	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	No
Comment:	There is no official IT Security team. The IT Staff manages all phases of IT. There are no documented roles and responsibilities.	

Governance 3		
Question:	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	No
Comment:	There are no privacy or retention policies in place. Human resources information and employee payroll inforation is sent offsite via SSL to Ultimate Software. HR data is stored and encrypted with Ultimate Software. The organization has a Cybersecurity Insurance policy in place that covers Cybersecurity incidents. Each of these are initial steps. A formal policy should be established outlining retention timelines based on regulatory requirements, privacy data should be identified and employees should have a clear understanding on what is privacy data, how it should be stored, processed, and destroyed.	

Governance 4

Question:	Governance and risk management processes address cybersecurity risks	No
Comment:	The IT departemnt does meet regularly with Executive leadership and discuss the current IT/Risk landscape and provide actionable plans for mitigating those risks. Risks are either accepted or authorized for mitigation at that time. There are no formal documents outlining the culture or dictating the approach for testing and managing risks.	

Risk Assessment 1		
Question:	Asset vulnerabilities are identified and documented	No
Comment:	Penetraiton tests are conducted yearly. A formal Vulnearbility Management Program does not exist.	

Risk Assessment 2		
Question:	Threat and vulnerability information is received from information sharing forums and sources	Yes
Comment:	Threat alerts are subscribed to from HackerNews and other sources. Alerts are reviewed internally within the team and action is taken accordingly.	

Risk Assessment 3		
Question:	Threats, both internal and external, are identified and documented	No
Comment:	Internal threats are not actively monitored and documented. A formal Vulnerability Management Program needs to be implemented. A local security Incident Response Team is not present and would need to be outsourced to an external vendor. Recommend formal Cybersecurity training for key personnel for incident response. Recommend acquiring IR retainer services for responding to security incidents.	

Risk Assessment 4		
Question:	Potential business impacts and likelihoods are identified	No
Comment:	No formal Risk Management Plan is in place. Recommend developing a System Security Plan and Continuous Monitroing Plan for full identification of organizational risk in order to make informative decisions on risk acceptance or mitigation.	

Risk Assessment 5		
Question:	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	No
Comment:	There's currently no formal risk management plan. All threats and vulnerabilities are handled in a reactive manner. No intrusion prevention services are being utilized. Recommend establishing a System Security Plan and continuous monitoring which would establish a formalized process for ongoing threat analysis.	

Risk Assessment 6		
Question:	Risk responses are identified and prioritized	No
Comment:	The organization lacks a formal risk mitigtaion strategy. Formal vulnerability management plan is not in place.	

Risk Management Strategy 1		
Question:	Risk management processes are established, managed, and agreed to by organizational stakeholders	No
Comment:	Risk Management Strategy is not in place. Recommend developing a System Security Plan (SSP).	

Risk Management Strategy 2		
Question:	Organizational risk tolerance is determined and clearly expressed	No
Comment:	Risk Management Strategy is not in place. Recommend developing a System Security Plan (SSP).	

Risk Management Strategy 3		
Question:	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	No
Comment:	A formal Risk Assessment is currently being performed for the first time in the organization and a Risk Management Program is currently at its infancy stage. Recommend initiation and alignment with a Risk Management Strategy in order to determine and be fully aware of the organization's risk tolerance.	

Access Control 1		
Question:	Identities and credentials are managed for authorized devices and users	No
Comment:	On-boarding of individuals are granted access based on their role. This information is provided by HR and their onboarding procedures. Username/password does not have to be changed by the user (not system-enforced). Passwords need to be changed after initial logon and every 3 months. Password complextiy is in place. Passwords appear in clear text digital documents and are also printed for delivery to the employee. HR initiates termination of employees and sends notification to IT, including day/time, email forwarding, etc. Devices are cleaned/wiped upon termination. Often there is miscommunication between HR and the field in regards to the termination process. A procedure needs to be formalized and streamlined. Recommend altering practice of including	

	clear text password of user accounts in digital or hard copy formats. Recommend forcing a password change after initial user logon and separating username ID and password upon delivery.

Access Control 2		
Question:	Physical access to assets is managed and protected	No
Comment:	Rear delivery door needs to be locked during the day. Access roles are not defined. Everyone has a 4-digit alarm code for entry. 30 security cameras in place. Doors are locked after hours. Security Alarm system will soon change. Recommend implementing a role-based access if possible or individual logged access.	

Access Control 3		
Question:	Remote access is managed	No
Comment:	RDP access is allowed from multiple locations from un-managed devices. VPN connections are limited. Three external developers are able to VPN into corporate test environment that still has access to production network. VPN connection is managed by the firewall.	

Access Control 4		
Question:	Access permissions are managed, incorporating the principles of least privilege and separation of duties	Yes
Comment:	AD templates for user rights are used for different roles (e.g., PM, RD, VP, Front Desk, etc.).	

Access Control 5		
Question:	Network integrity is protected, incorporating network segregation where appropriate	No
Comment:	Cameras and Wi-Fi network are separate networks from production. However, RDP access is allowed from multiple locations from un-managed devices. RDP access is mainly needed for JenARC and fileshares. Recommend moving JenARC to up-coming web-based front-end to remove need for RDP connections and segregate JenARC into its own VLAN. Also, move fileshare services to alternate solution (SharePoint, Box, OneDrive). Three external developers are able to VPN into corporate test environment that still have access to the production network. VPN is managed by the firewall. Recommend implementing a backup/redundant firewall.	

Awareness and Training 1		
Question:	All users are informed and trained	No
Comment:	All users are trained during onboarding. There is no annual training or any other formal decrees made by the employees stating that they understand security and the risks associated. The company is currently looking into KnowB4 and MediaPro as solution providers for ongoing training.	

Awareness and Training 2		
Question:	Privileged users understand roles & responsibilities	Yes
Comment:	There is currently no role-based training in place for priviliged users. The only priviliged users are the IT department. Based on the size of the department, all of IT has Domain Admin rights as they all perform cross-functional roles.	

Awareness and Training 3		
Question:	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	No
Comment:	IES (historical vendor), Jenarc, RSM (current GreatPlains accounting software vendor) and individual Mike Hanes (Jenarc contractor) all have remote access via RDP through the secure gateway and only have access to their particular server. There are no roles and responsibilites documents provided to the vendors or board members.	

Awareness and Training 4		
Question:	Senior executives understand roles & responsibilities	Yes
Comment:	Interview of senior executives hightlight their understanding of current security threats and their role and responsibility for protecting organizational assets, data and intellectual property.	

Awareness and Training 5		
Question:	Physical and information security personnel understand roles & responsibilities	Yes
Comment:	No physical security personnel is present in the environment. However, appropriate staff memebers are trained on security camera footage retrieval, door checks, and emergency situations.	

Data Security 1		
Question:	Data-at-rest is protected	No
Comment:	BitLocker is not active on endpoints. Un-encrypted drives are given to a charitable organization for data sanitization without full assurance of proper media sanitization. Organization does not have a Mobile Device Management (MDM) solution in place.	

Data Security 2		
Question:	Data-in-transit is protected	No
Comment:	RDP is used for external property employees without the use of a secure gateway. Only IT and Execs go through the secure gateway. Recommend implementing secure RDP gateway connection for all external users, or finding alternate solution for services provided via RDP. Recommend implementing VPN with current hardware capabilities.	

Data Security 3		
Question:	Assets are formally managed throughout removal, transfers, and disposition	No
Comment:	They use a charitable organization called Memory for Memory which claims they use NIST 800-88 guidelines for media sanitization. BitLocker is not implemented on these drives before the drives are removed from the environment. Data may include financial data and other data that may be used to compromise the system. Recommend implementing BitLocker or performing internal wipe of drives before using Memory for Memory service or repurposing of the drive.	

Data Security 4		
Question:	Adequate capacity to ensure availability is maintained	Yes
Comment:	PRTG (Paessler) is used to monitor network capacity requirements, drive space, memory, health, alerting, etc.	

Data Security 5		
Question:	Protections against data leaks are implemented	No
Comment:	External USB devices are allowed in the workstation environment. Recommend blocking USB ports for devices that do not need. Recommend confirming that SOPHOS is running scans on USB devices upon connection.	

Data Security 6		
Question:	Integrity checking mechanisms are used to verify software, firmware, and information integrity	No
Comment:	File integrity monitoring is not used. Automated notifications are not setup.	

Data Security 7		
Question:	The development and testing environment(s) are separate from the production environment	No
Comment:	Test environment is on a separate VLAN on Veeam. DevOps uses VPN to connect to Dev and Production servers. However, RDP is sometimes used by remote developers. Recommend disallowing RDP connections from remote locations.	

Information Protection Processes and Procedures 1		
Question:	A baseline configuration of information technology/industrial control systems is created and maintained	No
Comment:	Desktops are purchased from CDW and sent to Acme Inc.. New image is created annually and provided back to CDW. CDW sends all systems to Acme Inc. with the image pre-installed. All servers are built on-site. There are no standard build documents. Virtual environment build process is not documented.	

Information Protection Processes and Procedures 2		
Question:	A System Development Life Cycle to manage systems is implemented	No
Comment:	Currently not in place. Agile Development process is in place. Applicaitons do not undergo Static or Dynamic Application Security Testing (SAST and DAST). This is part of the roadmap for the futre of the organization. Recommend regular static and dynamic application testing during the development sprints.	

Information Protection Processes and Procedures 3		
Question:	Configuration change control processes are in place	No
Comment:	There is no Change Contorl Board (CCB) or Configuration Management (CM) policies in place. Recommend standing up a full CCB to discuss changes and introductions of new hardware and software into the environment. Recommend development of a CM Policy.	

Information Protection Processes and Procedures 4		
Question:	Backups of information are conducted, maintained, and tested periodically	No
Comment:	Backups are conducted daily. Archives occur monthly. Daily backups are stored locally and on external drives. Monthly backups are stored at AWS Glacier. Integrity testing of the backups is not performed at this time. Recommend scheduled testing of backup data integrity.	

Information Protection Processes and Procedures 5		
Question:	Policy and regulations regarding the physical operating environment for organizational assets are met	No
Comment:	The server room has no emergency lighting in place. The Emergency Power Off switch is located inside the room on the other side of the servers. This should be located immediately next to the exit door. Temperature sensors only exists in the server room. Two fire extinguishers are present but have expired. Wet pipe fire suppression is present in the server room. Recommend dry agent fire extinguishers that are kept current.	

Information Protection Processes and Procedures 6		
Question:	Data is destroyed according to policy	No
Comment:	No written data disposal policy is currently in place. Workstation drives are not formatted on-site before being provided to the charitable organization. Recommend implementing BitLocker to production drives and performing media sanitization before the drives are removed from the environment. Policies and procedures are not in place for disposal of data.	

Information Protection Processes and Procedures 7		
Question:	Protection processes are continuously improved	No
Comment:	The company has shown a progressive apporach to IT Security. Environment assessments are being conducted as a proactive measure. Penetration testing is performed annually. Executive branch has made a commitment to assigning assets and funding to improving the security posture of the organization. Recommend documenting auditable security requirements for ongoing monitoring of protection processes.	

Information Protection Processes and Procedures 8		
Question:	Effectiveness of protection technologies is shared with appropriate parties	Yes
Comment:	Acme Inc. has established a relationship with Digital Era Group to assist with the security roadmap. All IT personnel attend	

	training seminars/webinars at least once a year.

Information Protection Processes and Procedures 9		
Question:	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	No
Comment:	No Incident Response/Disaster Recovery plan currently in place. The organization relies on relationships wtih outside vendors.	

Information Protection Processes and Procedures 10		
Question:	Response and recovery plans are tested	No
Comment:	No COOP in place. Recommend development of a comprehensive COOP Plan and annual testing and review (e.g., tabletop exercises).	

Information Protection Processes and Procedures 11		
Question:	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Yes
Comment:	All employees are screened prior to receiving system access. No re-screening takes place.	

Information Protection Processes and Procedures 12		
Question:	A vulnerability management plan is developed and implemented	No
Comment:	Vulnerability Management Program is not in place. There is no formal process for ongoing scanning and remediation. Microsoft patches are pushed on a monthly basis through WSUS and are tested on a virtual test bed before deployment to the production environment. Recommend expanding the patching process to include additional vendors and developing a formal VM plan.	

Maintenance 1		
Question:	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	No

Comment:	Maintenance procedures need to be documented that include allowed personnel, activities, tools, etc. External vendors that may come in (e.g. Pitney Bowes) connect their laptops directly to printers that are connected to a production VLAN. Recommend implementing policy for virus and vulnerability scanning of external vendor hardware. Recommend placing printers in VLAN that is separate from endpoint clients.

Maintenance 2		
Question:	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	No
Comment:	Remote maintenance would only be performed by the IT Team. Remote maintenance occurs by establishing a secure connection via the RDP secure gateway. Remote access is not being logged. Records of maintenance activities are not documented. Recommend implementing logging capabilities.	

Protective Technology 1		
Question:	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	No
Comment:	No log monitoring or alerting is performed. Furthermore, there are no scheduled log reviews. Recommend a log aggregation tool with alerting or a full SIEM with aggregation and correlation.	

Protective Technology 2		
Question:	Removable media is protected and its use restricted according to policy	No
Comment:	Printers on-site employ a key fob. This design is meant to queue the data until the appropriate individual is able to retrieve the data from the printer. However, this feature is rarely used. Data centers and other digital media areas are protected by coded door locks. However, printed data is stored in the warehouse. This warehouse remains unlocked during the day and is accessible from the outside. The employees working in the warehouse have no authorization to view the material. Removable media is not tracked or encrypted. All USB ports are active.	

Protective Technology 3		
Question:	Access to systems and assets is controlled, incorporating the principle of least functionality	No
Comment:	With regards to the server environment, a few ports are disabled to keep outbound traffic from occuring in the event of a compromise. No physical ports are disabled. There is no File Integrity Monitoring (FIM) solution in place. Applicaiton whitelisting is not in use. Domain Administrator rights are being granted unnecessarily to SharePoint. Recommend exercising Least Privilege	

	principles across all devices, applications and users.

Protective Technology 4		
Question:	Communications and control networks are protected	No
Comment:	Remote access sessions are primarily initiated via RDP. Some mobile endpoints have enabled wireless access cards and are currently being disabled via a GPO and BIOS restriction. Recommend disabling any service that is not needed for a particular enduser to decrease attack surface. Recommend using VPN connection for external connections.	

Anomalies and Events 1		
Question:	A baseline of network operations and expected data flows for users and systems is established and managed	No
Comment:	A formal SSP is not present. Network diagrams and interconnections are not updated on a regular basis. A formal SIEM solution is not in place. Firewall configuration: Inbound ports for SFTP, HTTP, HTTP-S, RDP are allowed in. Outbound allows ports 80 and 443. Recommend formalizing an SSP after a full vulnerability assessment. Recommend regular updates of the network flow diagrams.	

Anomalies and Events 2		
Question:	Detected events are analyzed to understand attack targets and methods	No
Comment:	An automated solution for log aggregation and correlation is not present. Formal and active detection and analysis of targeted attacks and methods is not present in the environment.	

Anomalies and Events 3		
Question:	Event data are aggregated and correlated from multiple sources and sensors	No
Comment:	An automated solution for log aggregation and correlation is not present. Details regarding incidents are not being recorded in a repository for tracking and forensic purposes. Recommend implementing a log aggreation and correlation solution for active security monitoring of the environment.	

Anomalies and Events 4		
Question:	Impact of events is determined	No
Comment:	Root cause analysis is not being performed. Incident Response and Handling activities are able to be initiated, but additonal services would need to be outsourced.	

Anomalies and Events 5		
Question:	Incident alert thresholds are established	No
Comment:	A formal IRP is not present. Recommend drafting an incident response plan with metrics for alert thresholds.	

Security Continuous Monitoring 1		
Question:	The network is monitored to detect potential cybersecurity events	No
Comment:	There is currently no active monitoring or alerting in place for cybersecurity events.	

Security Continuous Monitoring 2		
Question:	The physical environment is monitored to detect potential cybersecurity events	No
Comment:	The physical environment is monitored 24x7. The door alarms are actively monitored and responses would occur at the time of the event. However, the cameras are not monitored and are used as support for investigations after the event has occurred. Insider threats are unable to be identified as all employees have an alarm security code and would not trigger an event.	

Security Continuous Monitoring 3		
Question:	Personnel activity is monitored to detect potential cybersecurity events	No
Comment:	No formal software invientory tracking occurs. PDQ inventories are occassionally pulled, but this is not performed for compliance auditing. Each user is issued a standard build. The end user has a limited account and is unable to install software without an administrator account.	

Security Continuous Monitoring 4		
Question:	Malicious code is detected	Yes
Comment:	Sophos immediately alerts the entire IT team. Real time scans are in place for all files. Additionally, there is a daily full scan scheduled. Recommend considering an endpoint protection solution that leverages Machine Learning and AI.	

Security Continuous Monitoring 5		
Question:	Unauthorized mobile code is detected	Yes
Comment:	Sophos performs remote code execution detection.	

Security Continuous Monitoring 6		
Question:	External service provider activity is monitored to detect potential cybersecurity events	No
Comment:	External service providers, when connecting to the environment, are locked into a sandbox environment with access only to those assets necessary to complete thier responsibilities. There is no monitoring of the activities or after-action reviews to guarantee only authorized activities were performed.	

Security Continuous Monitoring 7		
Question:	Monitoring for unauthorized personnel, connections, devices, and software is performed	No
Comment:	Unauthorized access, with the exception of the physical environment, are not monitored. There is currently no log monitoring occurring within the organization as no tool is available.	

Security Continuous Monitoring 8		
Question:	Vulnerability scans are performed	No
Comment:	Vulnerability scans are not performed. In addition to monthly patching of all applicable endpoints, recommend a full Vulnerability Management Program.	

Detection Processes 1		
Question:	Roles and responsibilities for detection are well defined to ensure accountability	Yes
Comment:	A formal Security Risk Assessment is currently being performed.	

Detection Processes 2

Question:	Detection activities comply with all applicable requirements	No
Comment:	A Continuous Monitoring Strategy and Vulnrability Management Program is not in place. A formal technical security control assessment has not been performed on the environment. Penetration tests have been performed. Recommend a formal Vulnerability Assessment be performed.	

Detection Processes 3		
Question:	Detection processes are tested	No
Comment:	A formal Security Assessment Report (SAR) is not present. Two penetrations tests are conducted per year. An independent third-party has been consulted for a formal Risk Assessment. Recommend drafting a formal SAR and ongoing assessment of risk within the organization.	

Detection Processes 4		
Question:	Event detection information is communicated to appropriate parties	No
Comment:	Limited notification of O365 events is being actively monitored. Also, SOPHOS, Mimecast, PRTG, and Veeam alert the IT Team of critical events. Recommend formal and comprehensive monthly vulnerability scans to be performed on the environment. Recommend considering introduction of a SIEM technology to provide a comprehensive view of the overall security posture based on log aggregation and correlation.	

Detection Processes 5		
Question:	Detection processes are continuously improved	No
Comment:	Penetration tests are performed twice a year. One penetration test is scheduled for the current year. Vulnerability scanning is not performed on a monthly basis. Recommend implementing a formal Vulnerability Management program for the environment.	

Response Planning 1		
Question:	Response plan is executed during or after an event	No
Comment:	Currently, the organization has no COOP. A Business Continuity Plan (BCP) and a Hurricane plan (C-CERT) is present. Recommend expanding the BCP to be a comprehensive COOP.	

Response Communications 1		
Question:	Personnel know their roles and order of operations when a response is needed	Yes
Comment:	In the existing C-CERT plan and BCP, all personnel are identified and understand their roles. However, this plan needs to be	

	expanded to include incidents other than natural disasters.

Response Communications 2		
Question:	Events are reported consistent with established criteria	No
Comment:	There is no documented incident response plan in place. The team understands the steps needed to react to an incident, but there is no documentation.	

Response Communications 3		
Question:	Information is shared consistent with response plans	No
Comment:	There is currently no contingency plan. However, the C-CERT plan and BCP is shared with the appropriate personnel.	

Response Communications 4		
Question:	Coordination with stakeholders occurs consistent with response plans	Yes
Comment:	The C-CERT Plan and BCP identifies key personnel and a call down tree.	

Response Communications 5		
Question:	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Yes
Comment:	In the event of an emergency, automated texts are sent out to notify the C-CERT team. Employees are instructed to visit the website for ongoing updates or they can dial into an 800 number.	

Analysis 1		
Question:	Notifications from detection systems are investigated	No
Comment:	Notifications are received throught the following products - PRTG (network, space, cpu, memory, health monitoring of the servers),	

	MimeCast (email alerts), Office365 (Office365 centric security events), Sophos (AV) and VEEAM (backup monitoring, low disk space). This a great first step in real-time monitoring. However, there is no log monitoring for intrusion activity. Recommend closing the gap and using an IDS and a log monitoring solution.

Analysis 2		
Question:	The impact of the incident is understood	Yes
Comment:	The organization has employed practices for actively monitoring bandwidth, monitoring outgoing employees, and has the means to analyze traffic in the event of an incident. Recommend implementation of an IDS/IPS solution.	

Analysis 3		
Question:	Forensics are performed	No
Comment:	There are no procedures or tools in place for performing Digital Forensics. There is no dedicated forensics team.	

Analysis 4		
Question:	Incidents are categorized consistent with response plans	No
Comment:	There is no Incident Response Plan (IRP). Recommend development of an Incident Repsonse Plan and IR Playbooks for critical incidents (e.g., ransomware and phishing incidents).	

Mitigation 1		
Question:	Incidents are contained	No
Comment:	There currently is no Incident Response Plan (IRP). Recommend incorporating steps for containment into a future IRP. Currently, all mitigations of incidents are performed by the IT Staff.	

Mitigation 2		
Question:	Incidents are mitigated	No

Comment:	There currently is no Incident Response Plan (IRP). Recommend incorporating steps for containment into a future IRP. Currently, all mitigations of incidents are performed by the IT Staff.

Mitigation 3		
Question:	Newly identified vulnerabilities are mitigated or documented as accepted risks	No
Comment:	The organization does not have nor employ a formal Vulnerability Management Program. Currently, the company mitigates all vulnerabilities that can be addressed through patching. However, in the event of EoL software, there is no tracking of assets throughout the organization. Examples given were Microsoft XP machines still in use due to older software that is still needed, and outdated versions of JAVA, among others.	

Response Improvements 1		
Question:	Response plans incorporate lessons learned	No
Comment:	There are currently no IRP. Recommend incorporating lessons learned into proposed IRP.	

Response Improvements 2		
Question:	Response strategies are updated	No
Comment:	There is currently no incident response or COOP. Recommend creating an annual review plan once the plan is created that will involve retesting of the plan and updating the plan based on lessons learned and the changing Cyber landscape.	

Recovery Planning 1		
Question:	Recovery plan is executed during or after an event	Yes
Comment:	During an incident that compromises availability of data, all business activities are redirectedd to Iland. Daily backups (Ransomware Recovery) are performed to a rolling set of USB Drives which will allow for recovery of all critical systems. Additionally, daily incremental backups are performed along with monthly full backups stored within AWS. Employees have roaming profiles stored on the server that are also backed up.	

Recovery Improvements 1		
Question:	Recovery plans incorporate lessons learned	No
Comment:	No recovery plans in place. Recommend creating recovery procedures and continuously updating these based on lessons learned and Cyber landscape.	

Recovery Improvements 2		
Question:	Recovery strategies are updated	No
Comment:	No recovery plans in place. Recommend creating recovery procedures and continuously updating these based on lessons learned and Cyber landscape.	

Recovery Communications 1		
Question:	Public relations are managed	No
Comment:	Public relations events are covered as part of the Cyber insurance policy. Non-public information is not being removed from drives that are being sent to Memory for Memory. Recommend media sanitization of the drives before sending to this organization. Additionally, it is recommended that BitLocker be implemented on all company drives, as permissible and feasible, for full Data at Rest (DAR) encryption.	

Recovery Communications 2		
Question:	Reputation after an event is repaired	Yes
Comment:	Active steps would be taken to recover from incidents that would compromise their reputation. Public relations events are covered as part of the Cyber insurance policy.	

Recovery Communications 3		
Question:	Recovery activities are communicated to internal stakeholders and executive and management teams	No
Comment:	Formal Contingency Plans are not present. The BCP and C-CERT do not constitute a comprehensive Contingency Plan. The BCP and C-CERT has been distributed to executives, stakeholders and DR personnel.	

Appendix A: Guidance

Information Security Roles

Typically, companies with 500 or fewer employees have an IT staffing ratio of about 1:18, while companies with 10,000 or more employees have a ratio of about 1:40.

The organization's senior management shall:

1. appoint or designate a senior-level information security official for the development, implementation and administration of security matters;
2. establish and communicate the organizations priorities for organizational mission, objectives and activities;
3. ensure that the organization's information security processes are in place, are communicated to all stakeholders, and consider and address organizational requirements;
4. formally assign an organization single point of contact or group to provide program oversight (governance), review and update the organizations security plan (strategy, policies, etc.), ensure compliance with the security plan by the workforce, and to evaluate and accept information security risk on behalf of the organization (e.g., CEO, COO, Security Steering Committee, etc.);
5. formulate, review, and approve information security policies and a policy exception process;
6. periodically, at a minimum annually, review and assess the effectiveness of the implementation of the information security policy;
7. provide clear direction and visible management support for security initiatives;
8. provide the resources needed for information security;
9. initiate plans and programs to maintain information security awareness;
10. ensure that all appropriate measures are taken to avoid cases of identity theft targeted at patients, employees and third parties;
11. ensure that the implementation of information security controls is coordinated across the organization; and
12. determine and coordinate, as needed, internal or external information security specialists, and review and coordinate results of the specialists' advice throughout the organization.
13. ensure that organization's information security strategy and goals are identified and considered, and address organizational specific requirements, and verify that appropriate processes are in place to meet the organization's strategy and goals;
14. formally review and approve in writing the establishment and administration of any information privacy, security and risk management programs;
15. formally approve in writing the assignment of specific roles and responsibilities for information security across the organization;
16. ensure the senior security official can demonstrate professional competency in security matters via a recognized security industry certification, appropriate vendor certifications or a minimum of eight (8) years of security-related experience;
17. document its risk acceptance process;
18. conduct an annual review (may be performed by a third party) of the effectiveness of its security program.

Information Security Policy Documents

As applicable to the focus of a particular document, policies shall contain:

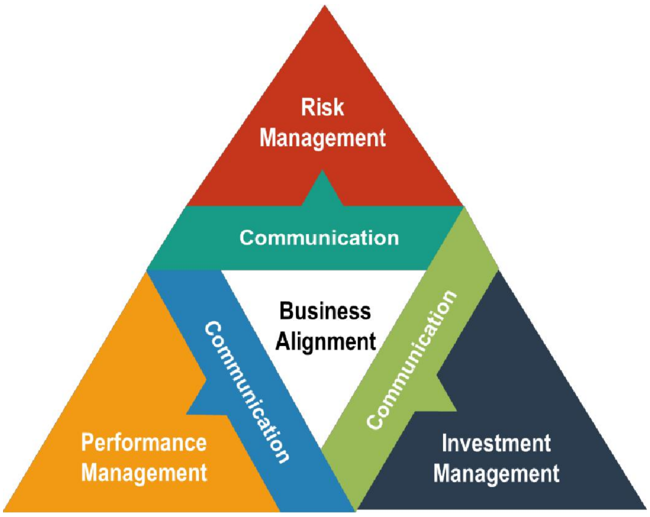
1. the organizations mission, vision, values, objectives, activities, and purpose, including the organizations place in critical infrastructure;
2. a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing;
3. a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
4. a framework for setting control objectives and controls, including the structure of risk assessment and risk management;
5. the need for information security;
6. the goals of information security;
7. compliance scope;
8. legislative, regulatory, and contractual requirements, including those for the protection of critical information and the legal and ethical responsibilities to protect this information;
9. arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination.
10. a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including but not limited to industry best practice control objectives such as:
11. compliance with legislative, regulatory, and contractual requirements;

    a. security education, training, and awareness requirements for the workforce, including researchers and research participants;
    b. incident response and business continuity management;
    c. consequences of information security policy violations;
    d. continuous monitoring;
    e. designating and maintaining an appropriately resourced and technically experienced information security team;
    f. physical security of areas where sensitive information (e.g., ePHI, PCI); and
    g. coordination among organizational entities;

12. a definition of general and specific responsibilities for information security management, including reporting information security incidents;
13. prescribes the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls; and
14. references to documentation, which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users shall comply with).

These information security policy documents shall be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

In the instance of any acquisitions, re-organizations, or mergers, or where the organization obtains support from third-party organizations or collaborates with third parties, and especially if these activities involve other jurisdictions, the policy framework shall include documented policy, controls and procedures that cover such interactions and that specify the responsibilities of all parties.



Information Security Strategic Plan

Drivers supporting an information security strategic plan include:

- integration of Risk Management, Performance Management, and Investment Management, and alignment with business objectives;
- defining consistent and integrated methodologies for design, development and implementation;
- detecting and resolving problems;
- reducing time to delivery from solution concept through implementation;
- provisioning flexible and adaptable architectures;
- proactively making decisions to more efficiently deliver results;
- eliminating redundancy to better support achievement of objectives;
- planning and managing human resources, relying on external expertise when required to augment internal staff;
- evolving into an organization where security is integrated as seamlessly as possible with applications, data, processes and workflows into a unified environment;
- ensuring that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
- employing a business case to record the resources required; and
- ensuring that information security resources are available for expenditure as planned.

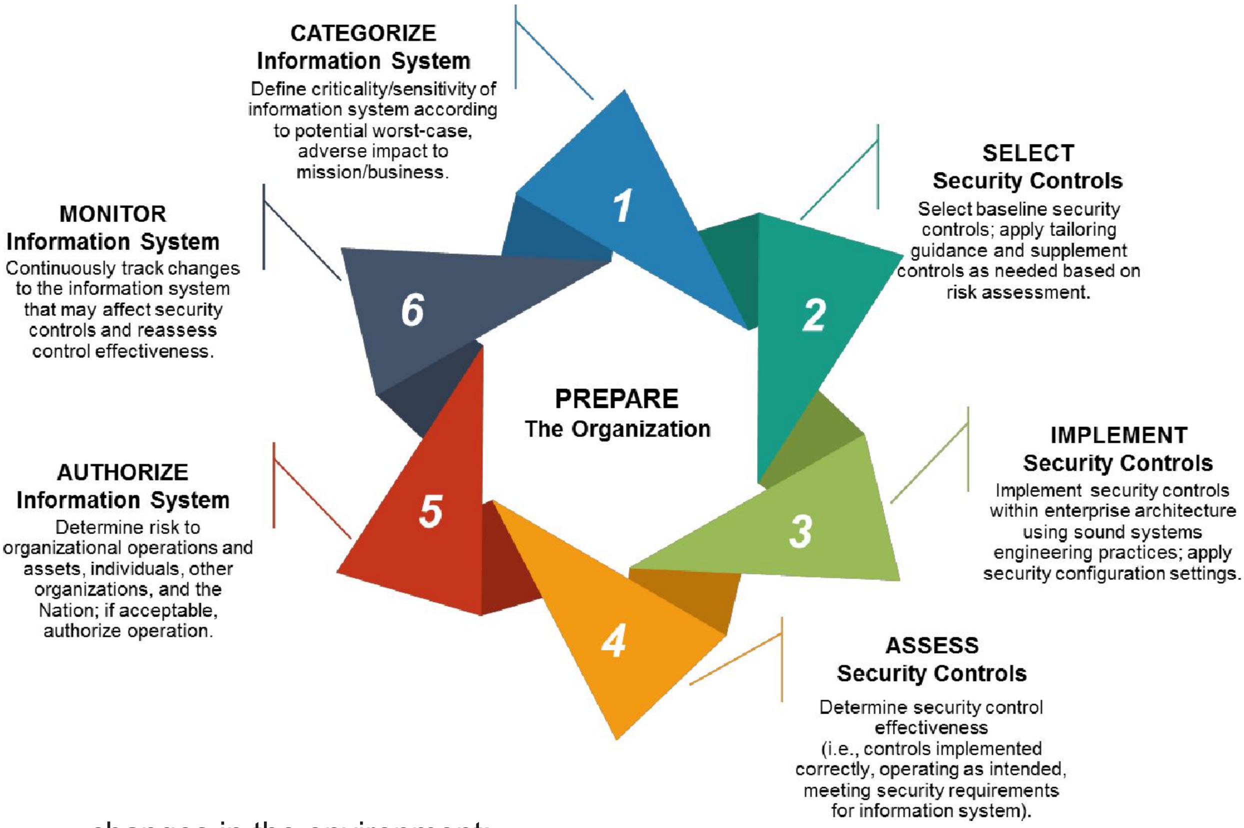
Risk Management Framework (RMF)

A comprehensive Risk Management Framework involves the continuous and proactive identification of Information Risk, including 3rd party, compliance and security risks, selection and implementation of remedial controls, monitoring and reporting on the state of Information Risk of the group to stakeholders including the Board of Directors.

Elements of the risk management program shall include:

1. the creation of a risk management policy for information systems and paper records that is formally approved by management and shall include:
    i. objectives of the risk management process;
    ii. management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and healthcare-specific risk analysis;
    iii. the connection between the risk management policy and the organization's strategic planning processes; and
    iv. documented risk assessment processes and procedures.

2. regular performance of risk assessments;
3. mitigation of risks identified from risk assessments and threat monitoring procedures;
4. risk tolerance thresholds are defined for each category of risk;
5. the plan for managing operational risk communicated to stakeholders;
6. reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk-level changes in the environment;


CATEGORIZE
Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.
SELECT
Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.
IMPLEMENT
Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.
ASSESS
Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).
AUTHORIZE
Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.
MONITOR
Information System
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
PREPARE
The Organization
1
2
3
4
5
6

7. repository and tracking system for risk assessments performed, and risk mitigation is completed or underway.
8. updating the risk management policy if any of these elements have changed;
9. repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually;
10. a dashboard for continuously reporting risk to stakeholders and the board.

The main steps of the RMF are:

- **Prepare** the organization to execute the RMF by considering a variety of organizational inputs that establish the context for managing security and privacy risk for the system-of-interest.
- **Categorize** the system and the information processed, stored, and transmitted by the system based on an impact analysis.

- Select an initial set of baseline security and privacy controls for the system and tailor the control baseline as needed based on an organizational assessment of risk and local conditions.
- **Implement** the security and privacy controls and describe how the controls are employed within the system and its environment of operation.
- **Assess** the security and privacy controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and enforcing security and privacy policy.
- **Authorize** the system or common controls based on a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation and the decision that this risk is acceptable.

- **Monitor** the system and the associated security and privacy controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting security and privacy impact analyses, and reporting the security and privacy state of the system.

The process of implementing RMF tasks may vary from organization to organization. The tasks are applied at appropriate phases in the system development life cycle. While the tasks appear in sequential order, there can be many points in the risk management process that require divergence from the sequential order including the need for iterative cycles between initial task execution and revisiting tasks. For example, security and privacy control assessment results can trigger a set of remediation actions by system owners and common control providers, which can in turn require the reassessment of selected controls.

There may also be other opportunities to diverge from the sequential nature of the tasks when it is more effective, efficient, or cost-effective to do so. Regardless of the task ordering, the final action before a system is placed into operation is the explicit acceptance of risk by the authorizing official.

Electronic Records Retention

The organization shall establish a formal record retention program that addresses:

1. the secure disposal of data (including data on disposed assets) when no longer needed for legal, regulatory, or business reasons, including disposal of personally identifiable information (tied to the data classification); and
2. a programmatic review process (automatic or manual) to identify and remove personally identifiable information that exceeds the requirements of the data retention policy on a quarterly basis.

Detailed procedures for record storage, access, retention, and destruction shall be implemented. In doing so, the following controls shall be implemented:

1. a retention schedule shall be drawn up identifying essential record types and the period of time for which they must be retained;
2. an inventory of sources of key information shall be maintained;

3. any related cryptographic keys shall be kept securely and made available only when necessary; and
4. any related cryptographic keying material and programs associated with encrypted archives or digital signatures shall also be stored to enable decryption of the records for the length of time the records are retained.

Identity & Access Management

Authentication of remote users shall be implemented via virtual private network (VPN) solutions that support a cryptographic-based technique, hardware tokens, or a challenge/response protocol. Dedicated private lines may also be used to provide assurance of the source of connections. Control all remote access through a limited number of managed access control points.

Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-up capabilities. Require callback capability with re-authentication to verify connections from authorized locations.

For application, systems and turnkey systems that require the vendor to log-on, the vendor shall be assigned a User ID and password and must enter the network through the standard authentication process. Access to such systems shall be authorized and logged. User IDs assigned to vendors will be reviewed in accordance with the organization's access review policy, at a minimum annually.

Node authentication may serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility.

Cryptographic techniques (e.g., based on machine certificates) can be used for ode authentication. This is part of several VPN based solutions.

The organization requires all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems, e.g., from an alternate work location or to sensitive information via a Web portal to use two-factor authentication.

Secure Logon Procedures

The procedure for logging into an operating system shall be designed to minimize the opportunity for unauthorized access. The log-on procedure shall therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.

The log-on procedures shall:

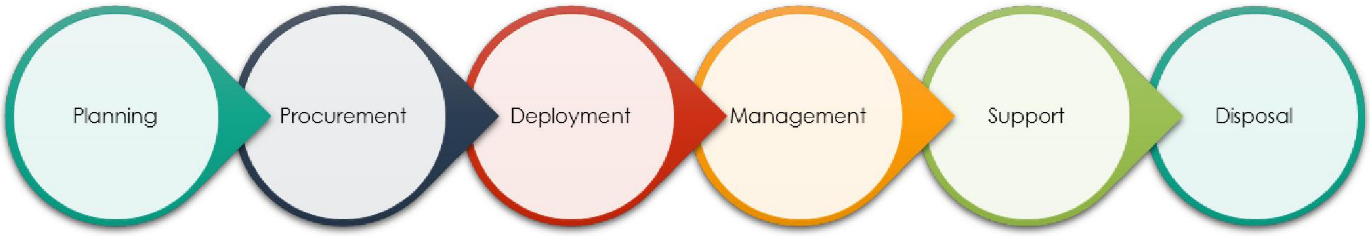
1. limit the number of unsuccessful log-on attempts allowed to three (3) attempts, and enforce:
   i. disconnecting data link connections;
   ii. sending an alarm message to the system console if the maximum number of log-on attempts is reached; and
   iii. setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected;
2. limit the maximum and minimum time allowed for the log-on procedure, if exceeded, the system shall terminate the log-on;
3. do not transmit usernames and passwords in clear text over the network;

4. do not display system or application identifiers until the log-on process has been successfully completed;
5. do not provide help messages during the log-on procedure that would aid an unauthorized user; and
6. validate the log-on information only on completion of all input data. If an error condition arises, the system shall not indicate which part of the data is correct or incorrect.

For more critical systems:

1. configure the system to lock out the user account automatically after three (3) failed log-on attempts by a user during a one (1) hour time period;
2. require the lock out to persist for a minimum of three (3) hours;
3. training shall include reporting procedures and responsibility for authorized users to report unauthorized log-ons and unauthorized attempts to log-on;
4. the number of concurrent sessions shall be limited to a specified number for all account types defined by the organization.

Asset Management



The organization shall identify and inventory all assets and services including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained or transmitted, including organizational and third-party sites, and document the importance of these assets. Locations in which PII constitutes a designated record set shall be explicitly identified in the asset inventory.

Approved bring your own device (BYOD) equipment shall also be included on the organizations inventories. The asset inventories shall also include all information necessary to recover from a disaster, including type or classification of the asset, format, location, backup information, license information, and the importance of these assets (business value). The inventory shall not duplicate other inventories unnecessarily, but it shall be ensured that the content is aligned.

The organization shall maintain an inventory of authorized wireless access points, including a documented business justification, to support unauthorized WAP identification.

Ownership, custodianship, and information classification shall be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection and sustainment commensurate with the importance of the assets shall be identified.

Specific policies shall exist for maintaining records of organizational property capital and non-capital) assigned to employees, contractors. Organization management shall be responsible for establishing procedures to issue and inventory property assigned to employees.

Records of property assigned to employees shall be reviewed and updated annually. The record shall be used to document and ensure that all property is returned to the organization upon employee termination or transfer out of the organization or department.

Organizations that assign organization-owned property to contractors shall ensure that the procedures for assigning and monitoring the use of the property are included in the contract.

The organization shall create and document the process/procedure the organization intends to use for deleting data from hard-drives prior to property transfer, exchange, or disposal/surplus. The organization shall create and document the process/procedure the organization intends to use to transfer, exchange or dispose of an IT-related asset (according to the organization's established lifecycle).

The asset inventory shall include all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device.

The inventory should include every system that has an Internet protocol (IP) address on the network including, but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc.

The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

The organization shall create, document, and maintain a process and procedure to physically inventory and reconcile IT asset inventory information on hand for:

1. capital assets (Inventory must be conducted at least annually)
2. non-capital assets

The asset inventory shall include:

1. unique identifier and/or serial number;
2. information system of which the component is a part;
3. type of information system component (e.g., server, desktop, application);
4. manufacturer/model information;
5. operating system type and version/service pack level;
6. presence of virtual machines;
7. application software version/license information;
8. physical location (e.g., building/room number);
9. logical location (e.g., IP address, position with the IS architecture);
10. media access control (MAC) address;
11. data ownership and custodian by position and role;
12. operational status;
13. primary and secondary administrators;
14. primary user; and
15. mapped organizational communications and data flows.

Threat and Vulnerability Management

The organization shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required.

Information resources (including tools and vulnerability mailing lists/other information sources), that will be used to identify relevant technical vulnerabilities and to maintain awareness about them, shall be identified for software and other technology (based on the asset inventory list).

These information resources shall be updated based on changes in the inventory, or when other new or useful resources are found.

Internal and external vulnerability assessments of sensitive information systems (e.g., systems containing critical information, cardholder data) and networked environments shall be performed on a quarterly basis, and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades), by a qualified individual. These tests shall include both network- and application-layer tests.

Security vulnerability assessment tools or services shall accommodate the virtualization technologies used by the organization (e.g., virtualization aware).

The action taken shall be carried out according to the controls related to change management or by following information security incident response procedures.

If a patch is available, change control procedures for the implementation of security patches and software modifications shall be followed.

This shall include assessing the risks associated with installing the patch (i.e., the risks posed by the vulnerability should be compared with the risk of installing the patch).

Patches shall be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated.

If no patch is available, is delayed, or not applied, other controls shall be applied including:

- documentation of impact;
- documented change approval by authorized parties;
- functionality testing to verify that the change does not adversely impact the security of the system;
- back-out procedures;
- turning off services or capabilities related to the vulnerability;
- adapting or adding access controls (e.g., firewalls) at network borders;
- increased monitoring to detect or prevent actual attacks; and
- raising awareness of the vulnerability.

An audit log shall be kept for all procedures undertaken.

Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. The risk ranking shall consider the CVSS score; classification of the vendor supplied patch, and/or the classification and criticality of the affected system. The technical vulnerability management process shall be evaluated on a quarterly basis in order to ensure its effectiveness and efficiency.

Systems at high risk shall be addressed first.

The organization's configuration standards shall be consistent with industry accepted system hardening standards, including:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS)
- National Institute of Standards Technology (NIST)

Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS 1.2 or later, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).

The organization conducts both internal and external penetration testing, within every three hundred sixty-five (365) days, on defined information systems or system components.

A prioritization process is implemented to determine which patches are applied across the organizations systems.

Patches installed in the production environment are also installed in the organizations disaster recovery environment in a timely manner.
Perform an enterprise security posture review annually.

The organization shall employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

Vulnerability scanning tools shall be updated regularly with all relevant information system vulnerabilities. The organization scans for vulnerabilities in the information system and hosted applications within every thirty (30) days and when new vulnerabilities potentially affecting the systems and networked environments are identified and reported.

The organization updates the list of information system vulnerabilities scanned at least weekly and when new vulnerabilities potentially affecting the systems and networked environments are identified and reported.

The organization includes privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities, to facilitate more thorough scanning.

The organization conducts regular penetration testing, no less than every three hundred sixty-five (365) days on defined information systems or system components, to identify vulnerabilities and attack vectors that can be used to successfully exploit enterprise systems. Penetration testing occurs from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization), as well as from within its boundaries (i.e., on the internal network), to simulate both outsider and insider attacks.

This includes tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.

The organization conducts regular penetration testing, no less than every three hundred sixty-five (365) days, on defined information systems or system components to identify vulnerabilities and attack vectors that can be used to successfully exploit enterprise systems. Penetration testing occurs from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks. This includes tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation. The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked). The organization reviews historic audit logs to determine high vulnerability scan findings identified in the information system has been previously exploited.

Appendix B: Artifacts Reviewed

The following list of artifacts were reviewed as a part of the Information Security Program Risk Assessment.

#	DOCUMENT NAME
1	C-CERT Response Plan
2	New Teammate Onboarding Guide
4	Backup Policy 2019
5	Acme Inc. Business Continuity Plan
6	Acme Inc. Employee Handbook