TPA Name

The Cerrado Standard

Cybersecurity Policies and Procedures

2022

TPA Name

Street Address

City, State and Zip

https://www.MYURL.com

Primary Contact

Contact Name

Contact Title

Revision History Table

Version	Date	Comments	Approved By
1.0	6/24/2022	Template Creation	MegaplanIT Holdings, LLC
1.1	11/16/2022	Terminology Updates, Minor Corrections	Ann Slotwinski
1.2	11/26/2022	Final Updates, Formatting Changes	Ann Slotwinski

Table of Contents

Acronyms and Abbreviations

CCPA	California Consumer Privacy Act
CCTV	Closed-Circuit Television
CDS	Change Detection Software
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
DMZ	Demilitarized Zone
EBSA	Employee Benefits Security Administration (US Department of Labor)
ERISA	Employee Retirement Income Security Act
FIM	File Integrity Monitoring
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HSM	hardware security module
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
ID	Identification
IPS	Intrusion Prevention System

IR	Incident Response
IT	Information Technology
MAC	Media Access Control Address
MDM	Mobile Device Management
NARA	The National Archives and Records Administration
NSA	National Security Agency
OWASP	The Open Web Application Security Project
PII	Personal Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
RBAC	Role-Based Access Control
SCD	Secure Cryptographic Device
SDLC	System Development Lifecycle and/or Software Development Lifecycle
TLS	Transport Layer Security
URL	Uniform Resource Locator
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

Overview and Policy Statement

The work we do in the retirement plan industry directly impacts plan sponsors and their participants' ability to comfortably retire. Record-keeping and the administration of retirement plans is complex, specialized work and the members of The Cerrado Group are committed to providing the best plan design, consulting and admistration possible. That includes the protection of the data we maintain. The effects of getting it wrong can be paralyzing in both the long and short term.

Plans covered under ERISA often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration (EBSA) has prepared a set of best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

The basis for a formal, well documented cybersecurity program is a set of information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the systems. EBSA has defined additional requirements for creating and maintaining strong information security policies, procedures, guidelines, and standards as follows.

Policies, Procedures, Guidelines, and Standards:

- Must be approved by senior leadership
- Must be reviewed at least annually, with updates as needed
- Must effectively explain terms to users
- Must be reviewed by an independent third-party assessor who confirms compliance
- Must document the specific framework(s) used to assess the security of its systems and practices
- Must have clearly defined roles and responsibilities for information security assignments
- Must be documented and implemented for the following information security areas:
    - Data governance and classification.
    - Access controls and identity management.
    - Business continuity and disaster recovery.
    - Configuration management.
    - Asset management.
    - Risk assessment.
    - Data disposal.
    - Incident response.
    - Systems operations.
    - Vulnerability and patch management.
    - System, application and network security and monitoring.
    - Systems and application development and performance.
    - Physical security and environmental controls.
    - Data privacy.

- Vendor and third-party service provider management.
- Consistent use of multi-factor authentication.
- Cybersecurity awareness training, which is given to all personnel annually.
- Encryption to protect all sensitive information transmitted and at rest.

The Cerrado Standard is provided by The Cerrado Group to address the required policies and framework selection needed to meet the EBSA cybersecurity program best practices. These policies have been written in clear language with the assistance of a third-party compliance assessment firm **based on the NIST Cybersecurity Framework (CSF).** In addition, all policies were reviewed and approved by The Cerrado Group management, are reviewed annually, and updated as appropriate.

Data Governance and Classification

Purpose

Data governance is a collection of data management practices and processes that help an enterprise manage its internal and external data flows. By implementing data governance, Third Party Admistration firms (TPAs) can improve data quality and help ensure the availability, usability, integrity, and security of its data assets. The purpose of classification is to break a subject into smaller, more manageable, more specific parts. Smaller subcategories help us make sense of the world, and the way in which these subcategories are created also helps us make sense of the world.

Data Governance

Executive sponsors will appoint data stewards, and through the establishment of data policies and Firm priorities, provide direction to them and data administrators. The following roles and responsibilities are recommended within Data Governance.

- **Executive Sponsor** – the senior manager responsible and accountable for major administrative data systems within their functional area.
- **Data Steward** - authorizes the use of data within their functional areas and monitors this use to verify appropriate data access.
- **Data Administrator** - works with the data stewards to establish procedures for the responsible management of data, including data entry and reporting

Data Access

The TPA Firm will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the relevant data steward to have an appropriate access level. Data access will be conducted in accordance with established policies.

Data Usage

TPA Firm personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to the security levels assigned to the data. Data usage falls into the categories of update, read-only, and external dissemination.

Authority to ***update*** data shall be granted by the appropriate data steward only to personnel whose job duties specify and require responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with the Firm's desire to provide excellent service to its plan participants.

Read-only usage to administrative information will be provided to employees for the support of TPA Firm business without unnecessary difficulties/restrictions.

Only those data elements classified as "public" can be externally ***disseminated*** for official or "nonofficial" reporting. Even release of directory information should be guided by the need to respect individual privacy and to protect the integrity of the data. The release of all other data must be approved by the responsible data steward.

Data Integrity and Integration

Data integrity refers to the validity, reliability, and accuracy of data. Data integrity relies on a clear understanding of the business processes underlying the data and the consistent definition of each data element.

Data integration, or the ability of data to be assimilated across information systems, is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

All employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate data stewards or senior management.

Data Classification

TPA Firm data shall be classified using the following information classification levels:

- **Restricted**: Information that must be protected from unauthorized access, modification and/or destruction in accordance with regulation, law, and/or company policy.
- **Confidential**: Information that is not Restricted but must be protected from unauthorized access, modification and/or destruction because it has a high risk of causing reputational or other harm to the TPA Firm if not properly protected.
- **Internal**: Information that does not rise to the level of Confidential but is not intended for public use.
- **Public**: Information that may be freely shared with the public.

Information protection and information handling requirements for TPA Firms, including requirements for specific data elements such as personally identifiable information (PII) and other sensitive information are included in the Information Protection and Asset Management Standard. Authorized users are required to comply with all laws and regulations regarding the privacy of PII in employment and customer relationships.

Information governance controls shall be in place to properly inventory and classify information, including defining the information and understanding the uses of the information and its flow through systems. In addition, controls shall be in place to ensure information is balanced and access is managed in order to protect the information and ensure that the quality of the information remains intact.

References

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Data Privacy

Purpose

Data Privacy or Information privacy is a part of the data protection area that deals with the proper handling of data focusing on compliance with data protection regulations. Data Privacy is centered around how data should be collected, stored, managed, and shared with any third parties, as well as compliance with the applicable privacy laws (such as California Consumer Privacy Act-CCPA or General Data Protection Regulation GDPR).

This data security policy applies all customer data, personal data, or other Firm data defined as sensitive by the Firm's data classification policy. Therefore, it applies to every server, database, and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with the Firm's IT services is also subject to this policy.

Firm Responsibilities

The TPA Firm shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

- Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.
- The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.
- Management must ensure each user understands this data security policy and the login and logoff guidelines and may require formal acknowledgement that the user understands the conditions of access.
- Records of user access may be used to provide evidence for security incident investigations.
- Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

User Responsibilities

- All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
- All users must keep their workplace clear of any sensitive or confidential information when they leave.
- All users must keep their passwords confidential and not share them.

It is the responsibility of all TPA Firm employees to be aware of how personal information is being processed in their area and to immediately report suspected or actual unauthorized access or disclosure of any sensitive data to senior management.

Privacy Statements

Privacy statements (also known as privacy notices) are important documents which disclose ways a party collects, stores, uses and discloses an individual's data. They are intended to provide an individual insight into the collection, use, disclosure, and protection of their personal information (PI).

If the TPA Firm processes an individual's PI, the department or a resource representing the department must prepare and provide a privacy statement.

The privacy statements must be reviewed by senior management at creation, and annually, thereafter, or any time there is a change in the way in which the TPA Firm is using the individual's PI. If a change to a privacy statement applies to data already collected (under a previous privacy statement), then the department must give the individual the opportunity to acknowledge the change.

The privacy statement includes detail on what is collected, why it is collected, what is done with the information, and any rights the TPA Firm has over the data. It includes detail on how an individual can request changes to their PI if the PI is inaccurate. The department must provide privacy statements to individuals whose PI is collected by the TPA Firm before or at the time of collection when providing products and services.

Each department must maintain an inventory of their privacy statements, and senior management reviews and provides final signoff before publishing.

Reporting Privacy Concerns or Incidents

A privacy incident is an event in which personal information may have been accessed, used, or disclosed without authorization.

Authorized users are required to immediately report any privacy concerns or suspected incidents, whether inadvertent or intentional. Prompt reporting of all suspected incidents allows the TPA Firm to investigate and report any incident as required by federal and state laws and regulations.

The TPA Firm offers various ways in which a person can report a potential privacy incident:

- Contact immediate manager.
- Upon notification from an employee regarding an incident, managers must immediately notify senior management.

References

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Access Controls and Identity Management

Purpose

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to IT systems and data. Identity proofing establishes that a subject is who they claim to be. Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity. For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as that which accessed the service previously. Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individual subjects over an open network to access digital services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks.

Access Control

Access control mainly consists of two components: authentication and authorization. The TPA Firm will ensure that Access Control systems adhere to the following conditions for purposes of complying with the US Department of Labor Employee Benefits Security Administration Cybersecurity Program Best Practices:

1. Access to systems, assets and associated facilities is limited to authorized users, processes, devices, activities, and transactions.
2. Access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) are limited based on the role of the individual and adhere to the need-to-access principle.
3. Access controls are implemented via an automated access control system.
4. Access control systems are in place on all system components.
5. Access control systems have a default Deny All setting.
6. Access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with standard operating procedures.
7. All employees use unique, complex passwords.

8. Multi-factor authentication is used wherever possible, especially to access the internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control methodology.
9. Policies, procedures, and controls are implemented to monitor the activity of authorized users and detect unauthorized access, use of, or tampering with, nonpublic information.
10. Procedures are implemented to ensure that any sensitive information about a participant or beneficiary in the service provider's records matches the information that the plan maintains about the participant.
11. Access controls are used to confirm the identity of the authorized recipient of the funds.
12. An authorization form is required for all access, which must specify required privileges, must validate the user's identity, and must be signed by management.
13. Prohibit direct public access between the Internet and any system component in the PII environment.

Access controls must be configured and operational to track all access to data – including the user's identity, time and date, and a listing of the accessed data. This system of controls protects sensitive data and ensures that the information is not improperly distributed, copied, modified, or deleted.

Access to network systems and data must be limited to those employees who have been properly authorized. As such, the TPA Firm adheres to the concept of Role-Based Access Control (RBAC), which results in users being assigned privileges based on a job classification or function. Each user will be authorized to view a certain classification level. All access must be configured to authorize only the data each user needs for their specific position or business role. Every user must be authorized to access the TPA Firm's systems. Authorization pertains to the user's business role and will only be authorized when necessary to fulfill said role.

Authorized TPA Firm personnel will be responsible for the addition, deletion, and modification of user IDs and credentials. Any TPA Firm employees or vendors that have network access must have that access immediately revoked once their relationship with the TPA Firm is severed for any reason.

Identity Management

For employees who require access to confidential, sensitive, or private information, the data access request process must be followed. First, all requests must be approved by the Information Security Department. Second, the user must file a completed

Authorization Request Form. Any employee who requests access to data above their normal security clearance must follow this procedure, as well as provide documentation that reports their access source and access time limits.

This is the general workflow for requesting access to data:

1. User requests authorization by submitting an Authorization Request Form.
2. User's manager must approve the request based on the employee's role. The manager must make note of any additional access requirements before handing the request off to the Information Security Department.
3. The Information Security Department will coordinate with relevant department managers to ensure that the user is qualified to access to their data.
4. The Information Security Department will then hand the request off to the System Administrator.
5. The System Administrator will create or modify the user's account, inform the user's manager, and forward that information to the Human Resources Department. Human Resources will then include these credentials within the user's employee file.
6. User's manager will inform the user that the request has been completed or denied.

Each authorized user will be given a unique account name. The user will create a secret password, utilizing the comprehensive password parameters put in place by the TPA Firm. In addition, all TPA Firm systems must authenticate via passwords.

Multi-Factor Authentication

Multi-factor authentication, along with encryption to protect data in transit, must be used consistently under the following conditions:

- All access (local, network, or remote) by privileged or administrative accounts.
- All remote network access originating from outside the TPA Firm's network.
- All non-console access into the TPA Firm's network for personnel with administrative access.
- All management of network devices.

The above requirements apply to TPA Firm employees and third-party vendors. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. TPA Firms can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Two-factor authentication is the most common form of multi-factor authentication used and employs two of the three following authentication methods:

1. Something you know (example: password or passphrase)
2. Something you have (example: soft or hard tokens, smart card or valid and unique digital certificate installed on user's workstation)
3. Something you are (example: biometric)

It is not acceptable to employ one of these methods twice. For example, requiring a user to enter two different passwords does not constitute two-factor authentication.

Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards. In addition to authenticating users at the system level (i.e., at logon), TPA Firms may employ authentication mechanisms at the application level, at their discretion, to provide increased security.

Third-Party Access

Authorized TPA Firm personnel will actively manage those IDs used by third-party vendors as follows:

- Vendor access will be enabled only during the time period needed and disabled when not in use.
- Vendor access will be intently monitored when in use by all appropriate means.
- Vendor access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) are limited based on the role of the individual and adhere to the need-to-access principle.

- Vendor access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with policy.
- Vendor network access must be immediately revoked once their relationship with the TPA Firm is severed for any reason.

Password Requirements

User-level access must include authentication measures, such as a password. Non-authenticated user IDs, shared IDs, and group IDs are not permitted.

Each TPA Firm system must employ an automated access control process. This process will:

- Require passwords of at least 12 characters, which include a combination of both numbers and letters.
- Conduct internal reviews every 90 days to ensure that only active employees have active credentials.
- Authenticate every account (meaning all users, systems, and applications) with a password.
- Identify every user by their unique account name.
- Mandate that a user account will be locked out of the system after five failed attempts to connect. The account will remain locked for at least 30 minutes or until a Systems Administrator unlocks it.
- Require that new passwords not be the same as the previous four passwords.
- Mandate that all new and reset passwords be unique and require the user to change it upon first use.
- Require passwords to be changed every 90 days.
- Require that the system disconnect a user after an idle time of 15 minutes.

In addition, TPA Firms should:

- Encourage use of a passphrase comprised of unrelated words.
- Encourage users to check the strength of their password and adjust as needed https://thycotic.com/resources/password-strength-checker/

While this process applies to the authentication of all TPA Firm and third-party vendor users, any customer utilizing a TPA Firm system must also adhere to these requirements.

Individuals granted network access for the first time and individuals requesting a password reset must be granted a unique password that must be changed after first use. Furthermore, for all non-face-to-face password-reset requests, the System Administrator must verify the user's identity.

Passwords stored in any system components within the environment or that are transmitted over the network must be rendered unreadable at all times using strong cryptography.

References

NIST CSF PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes

NIST CSF PR.AC-3: Remote access is managed

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

NIST CSF 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)

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Business Continuity and Disaster Recovery

Purpose

Business continuity is a proactive way to ensure mission-critical operations proceed during a disruption. A comprehensive plan includes contact information, steps for what to do when faced with a variety of incidents and a guide for when to use the document. A disaster recovery plan is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber-attacks, and any other disruptive events. The plan contains strategies on minimizing the effects of a disaster, helping an organization to quickly resume key operations or continue to operate as if there was no disruption.

Business Resiliency Program

Business resilience is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data. An effective Business Resiliency Program should:

- Reasonably define the internal processes for responding to a cybersecurity event or disaster.
- Reasonably define plan goals.
- Define the documentation and reporting requirements regarding cybersecurity events and responses.
- Clearly define and describe the roles, responsibilities, and authority levels.
- Describe external and internal communications and information sharing, including protocols to notify plan sponsor and other affected user(s) if needed.
- Identify remediation plans for any identified weaknesses in information systems.
- Include after action reports that discuss how plans will be evaluated and updated following a cybersecurity event or disaster.
- Be annually tested based on possible risk scenarios.

The core components of a program include the Business Continuity Plan, Disaster Recovery Plan, and Incident Response Plan.

Business Continuity Plan

The Business Continuity Plan is the written set of procedures an organization follows to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels following a disruption. The Business Continuity Plan should include the following elements:

- Risks and potential business impact
- Planning an effective response
- Roles and responsibilities
- Communications
- Testing and training

Disaster Recovery Plan

The Disaster Recovery Plan is the documented process to recover and resume an organization's IT infrastructure, business applications, and data services in the event of a major disruption. The Disaster Recovery Plan should include the following elements:

- Objective and Scope
- Personnel
- Software Application Inventory
- Hardware Inventory
- Backup Procedures
    - Inventory of data required
    - RPO/RTO as acceptable
- Declaring a Disaster
- Recovery Procedures
    - Mobile Site
    - Hot Site

    - Cold Site
- Restoring the System to Normal Operations
- Documentation Requirements
- Communications
- Testing and Training
- Revision History

Incident Response Plan

The Incident Response Plan is a set of instructions to help IT staff detect, respond to, and recover from security incidents. The Incident Response Plan should include the following elements:

- Preparation
- Detection
- Analysis Containment
- Eradication
- Recovery
- Communications
- Post-incident activity

For additional information for creating and implementing an Incident Response Plan reference NIST 800-61

References

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

RC.RP-1: Recovery plan is executed during or after a cybersecurity incident

RC.IM-1: Recovery plans incorporate lessons learned

RC.IM-2: Recovery strategies are updated

RC.CO-1: Public relations are managed

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Configuration Management

Purpose

The role of configuration management is to maintain systems in a desired state. Traditionally, this was handled manually or with custom scripting by system administrators. Automation is the use of software to perform tasks, such as configuration management, in order to reduce cost, complexity, and errors.

Strong Technical Controls Implementing Best Security Practices.

Technical security solutions are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. Best security practices for technical security include:

- Ensuring all hardware, software, and firmware models and versions are kept up to date
    - See Vulnerability and Patch Management Policy
- Vendor-supported firewalls, intrusion detection and prevention appliances/tools
- Regularly updating antivirus software
    - See System, Application, and Network Security Policy
- Applying patches in a timely manner (preferably automated)
    - See Vulnerability and Patch Management Policy
- Segmenting sensitive resources on the Network from non-sensitive resources
- Deploying only hardened System configurations
- Conducting routine data backup (preferably automated)

Firewall

Establish and implement firewall and router configuration standards that:

- Formalizes testing whenever configurations change

- Identifies all connections between the environment and other networks (including wireless) with documentation and diagrams
- Documents business justification and various technical settings for each implementation
- Diagrams all sensitive data flows across systems and networks
- Stipulates a review of configuration rule sets at least once every six months

Build firewall and router configurations that restrict all traffic, inbound and outbound, from “untrusted” networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the environment.

Install personal firewall software or equivalent functionality on any devices (including company and/or employee owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the environment.

IDS/IPS

- Intrusion Detection System: An IDS is designed to detect a potential incident and generate an alert but will not prevent the incident from occurring. While this may seem inferior to an IPS, it may be a good solution for systems with high availability requirements and critical infrastructure. For these systems, the most important thing is that the systems continue running and the blocking of suspicious (and potentially malicious) traffic may impact their operations. Notifying a human operator of the issue enables them to evaluate the situation and make an informed decision on how to respond.
- Intrusion Prevention System: An IPS, on the other hand, is designed to take action to block anything that it believes to be a threat to the protected system. As malware attacks become faster and more sophisticated, this is a useful capability because it limits the potential damage than an attack can cause. An IPS is ideal for environments where any intrusion could cause significant damage, such as databases containing sensitive data. An IPS is typically a signature or behavior-based network appliance which monitors network connections and traffic. The device analyzes the patterns or transmissions of the traffic against its signature base or behavior analytics. From there a judgement is made by the device to block or allow the traffic flow being monitored.
- IDS and IPS both have their advantages and disadvantages. When selecting a system for a potential use case, it is important to consider the tradeoffs between system availability and usability and the need for protection. An IDS leaves a window for an

attacker to cause damage to a target system, while a false positive detection by an IPS can negatively impact system usability.

Segmentation

All inbound Internet traffic must use a network segmented by a firewall. This segmented zone is known as the "Demilitarized Zone" (DMZ), which adds an additional layer of network security between the Internet and the TPA Firm's internal networks so that external entities only have direct connections to devices in the DMZ and not the entire internal network. This inbound traffic must be limited to only those ports deemed necessary for TPA Firm business. Any TPA Firm databases or directories storing client data must be stored on an internal network that is segmented from the DMZ network. With the exception of the DMZ, perimeter routers should never be configured to include a route to internal address space.

Hardening Standards

TPA Firms must adopt configuration standards for all system components which must be maintained in accordance with industry-accepted system hardening standards. The TPA Firm shall develop and maintain system hardening standards based on one or a combination of the following sources:

- CIS Benchmarks
- SANS
- NIST
- DOD STIGS

Backup and Recovery

TPA Firm performs weekly backups of user-level and system-level information along with system documentation, configurations, and settings. These backups are secured to protect the confidentiality, integrity, and availability of the backup information. All critical information is stored on specially marked media and kept at an alternate storage site. Backup media is tested monthly to verify the media reliability and information integrity. Any media found to be deficient is immediately replaced and old media destroyed per the Data Disposal Policy.

Deletion or destruction of backup information requires dual authorization to prevent accidental or malicious destruction of critical files. All backup files must be protected with strong cryptography and no single person shall have knowledge of or access to the full encryption key.

References

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

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

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Asset Management

Purpose

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal investigations, and insurance activities.

Any and all data assets stored on TPA Firm systems that are classified as Restricted or Confidential must adhere to this policy.

Asset Inventory

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

At a minimum, the follow asset types are subject to tracking and asset tagging:

- Desktops and Laptops
- Firm-owned Mobile Devices (Phones, Tablets, etc.)
- Printers, copiers, fax machines, and multifunction print devices
- Servers
- Network appliances (e.g., firewalls, routers, switches, etc.)
- Private Branch Exchange (PBX) and Voice over Internet Protocol (VOIP) Telephony Systems and Components
- Internet Protocol (IP) Enabled Video and Security Devices
- Removable Media (Memory devices, external hard drives, etc.)

Prior to deployment, the asset information must be entered into the asset tracking system (Excel spreadsheet, database, etc.). All assets maintained in the asset tracking system inventory shall have an assigned owner. The asset-tracking system, must minimally include the following elements for properly documenting the asset inventory:

- Type of asset – Firewall, routers, switches, server (physical and or/logical, etc.)
- Make and model (hardware) / version number (software)
- Primary function
- Serial number
- MAC address
- Physical and/or virtual location
- Owner / Primary User
- Department
- Disposition (In Service, Out for Repair, Decommissioned, etc.)

Mobile Device Management

The primary goal of Mobile Device Management (MDM) is to protect the integrity of the confidential client and business data that resides within the TPA Firm's technology infrastructure, including internal and external cloud services. The intent is to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unauthorized resources. A breach of this type may result in loss of information, damage to critical applications, loss of revenue, damage the company's public image, breach our data privacy requirements, and violate data privacy laws. Therefore, all employees, contractors, or personnel using a mobile device connected to the Firm's corporate network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to company-defined processes and policies in doing so.

This policy applies to all employees, including full and part-time staff, contractors, freelancers, and other agents who use any mobile device to access, store, backup, or relocate any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of trust the Firm has built with its clients, supply chain partners, and other constituents. Consequently, employment does not automatically guarantee the initial or ongoing ability to use these devices to gain access to corporate networks and information.

- Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password; a PIN is not sufficient. All data stored on the device must be encrypted using strong encryption. See password and encryption policy for additional background. Employees agree never to disclose their passwords to anyone.

- All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.
- Any non-corporate computers used to synchronize or backup data on mobile devices will have installed up-to-date antivirus and anti-malware software deemed necessary.
- Passwords and other confidential data are not to be stored unencrypted on mobile devices.
- Any mobile device that is being used to store or access Firm data must adhere to the authentication requirements. In addition, all hardware security configurations must be pre-approved by the TPA Firm before any enterprise data-carrying device can be connected to the corporate network.
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with the TPA Firm's overarching security policy.
- Employees, contractors, and temporary staff accessing Firm internet resources from a smartphone or tablet will NOT save their user credentials or internet sessions when logging in or accessing company resources of any kind.
- Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once its use is no longer required.
- In the event of a lost or stolen mobile device, the user is required to report the incident to IT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to company business or personal. The Remote Wipe Waiver, which ensures that the user understands that personal data may be erased in the rare event of a security breach, must be agreed to before connecting the device to corporate resources.
- Usage of location-based services and mobile check-in services, which use GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.
- Usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.
- Applications that are not approved by IT are not to be used within the workplace or in conjunction with corporate data.

Asset Disposal and Repurposing

Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport, or surplus.

When disposing of any asset, sensitive data must be removed prior to disposal. See Data Disposal Policy for additional guidance on sanitizing data.

References

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

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

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

ID.AM-4: External information systems are catalogued

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Risk Assessment

Purpose

The purpose of this policy is to ensure the TPA Firm understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. A Risk Assessment is an effort to identify, estimate, and prioritize information system risks. IT threats are constantly changing, so it is important to design a manageable, effective risk assessment schedule. This policy establishes the framework for a formal risk management program by designating responsibility for risk identification and analysis, planning for risk mitigation, and outlining program management and oversight. Program management and oversight is a Firm-wide responsibility that calls for the active involvement of executive leadership, departmental management, data stewards, and others involved in decision-making concerning risks.

Overview

Risks to the TPA Firm are identified, considered, and managed in order to support effective operation of the Firm. Organizations should codify the risk assessment's scope, methodology, and frequency. A risk assessment should:

- Identify, assess, and document how identified cybersecurity risks or threats are evaluated and categorized
- Establish criteria to evaluate the confidentiality, integrity, and availability of the information systems and nonpublic information, and document how existing controls address the identified risks
- Describe how the cybersecurity program will mitigate or accept the risks identified
- Facilitate the revision of controls resulting from changes in technology and emerging threats
- Be kept current to account for changes to information systems, nonpublic information, or business operations.

The TPA Firm will designate a Senior Manager to manage the risk assessment policy and procedures. The Senior Manager is responsible to:

- Review and update the risk assessment procedures on an annual basis,

- Ensure that the risk assessment procedures implement the risk assessment policy and controls, and
- Develop, document, and implement remediation actions for violations of the risk assessment policy.

The TPA Firm will engage in a risk assessment process that is performed at least annually and upon significant changes to their environment. This assessment process will identify critical assets, threats, and vulnerabilities, and will result in a formal, documented analysis of risk. Annual risk assessments are conducted to evaluate the level of risk, including the likelihood and impact, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.

The risk assessment must consider risks posed to the TPA Firm's operations, assets, or individuals from external parties, including but not limited to the following:

- Contractors operating information systems on behalf of TPA Firm
- Individuals accessing the TPA Firm's information systems

One or more tasks to remediate a finding must be documented in an Action Plan (Risk Register, POA&M, CAP, etc.) for any of the following:

- Critical-level risks that are not remediated within 7 days
- High-level risks that are not corrected within 21 days
- Medium-level risks that are not corrected within 30 days
- Low level risks that are not corrected within 90 days

All assessment results will be provided to management within thirty (30) days of completion.

Risk Assessment/Analysis

Risk assessment or analysis is the act of determining the probability that a risk will occur and the impact that event would have if it did occur. This analyzes the cause and effect of each possible event. Once risks have been identified and documented, risk analysis must be performed. During the risk analysis process, each potential risk event will be evaluated for the following:

- The probability that the risk will occur
- The impact of the risk if it occurs

These two factors of assessing the risk involving probability and impact shall be measured for probability using a scale of Low, Medium, and High, and giving each an associated number. For impact, TPA Firms shall use a qualitative method for analysis as it is typically a quicker and usually more cost-effective way to analyze risks. Analysis will be performed with the goal of gathering data on the following:

- The likelihood of the risk occurring
- The qualitative impact on the company, system, or data
- The quality of the risk data being utilized

The TPA Firm shall implement a suite of automated monitoring tools to effectively monitor and identify vulnerabilities for inclusion in the risk analysis on networked computer servers and workstations.

Impact Definitions

- **High**
  - If an event could be expected to have a severe or catastrophic adverse effect on the TPA Firm operations, assets, or individuals; and cause a loss of business mission capability for a period that poses a threat to human life, or results in a loss of major assets.

- **Moderate**
    - If an event could be expected to have a serious adverse effect on TPA Firm operations, assets, or individuals, and cause significant degradation in business mission capability, place the TPA Firm at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.
- **Low**
    - If an event could be expected to have a limited adverse effect on TPA Firm operations (including business mission, functions, image or reputation, assets, or individuals); and cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.

Risk Response

For each identified risk, a response must be identified. The Senior Manager or Risk Committee Members will select a risk response for each risk. The likelihood and impact of the risk will be the basis of recommending which actions should be taken to mitigate the risk. During response planning, strategies and plans are developed to minimize the effects of the risk to a point where the risk can be controlled and managed.

- **Avoid**: Risk avoidance involves changing aspects of the overall business process or system architecture to eliminate the threat.
- **Transfer**: Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat it simply makes another party responsible for managing it. This would include identifying avenues of insurance, etc.
- **Mitigate**: Risk mitigation involves reducing the probability and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans are examples of risk mitigation.
- **Accept**: Risk acceptance should normally only be taken for low-priority risks. All risks should have a recommendation of control(s) and / or alternative solutions to mitigate risk.

Use of Independent Assessors

When assessments must be conducted by an entity with an explicitly determined degree of independence to the organization, independence must be determined by Senior Management based on the security categorization of the information system and/or the risk to TPA Firm operations and assets, and to individuals. To make an informed, risk-based decision, the selection of independent assessors must consider the following criteria to ensure credibility of the security assessment results and to receive the most objective information possible. Preserving the impartial and unbiased nature of the assessment process including, but not limited to, freedom from any perceived or actual conflicts of interest with respect to the following:

- The development, operation, and/or management of the information system
- The chain of command associated with the information system
- The determination of security control effectiveness
- A competitive relationship with any organization associated with the information system being assessed or impacts on their reputations
- Undue influence as a result of a contractual or other related relationship
- The assessor's technical expertise and knowledge of State and federal compliance standards

References

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

ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources

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

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

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

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

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

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

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

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Data Retention and Disposal

Purpose

The purpose of this policy is to provide for proper cleaning or destruction of sensitive/confidential data and licensed software on all computer systems, electronic devices, and electronic media being disposed, recycled, or transferred either as surplus property or to another user. The sanitization process must remove information from system media such that the information cannot be retrieved or reconstructed.

Data Retention

Any and all data assets stored on TPA Firm systems that are classified as sensitive or confidential must adhere to this policy. The data creator or authorized manager must establish a specific retention timeframe for any sensitive or confidential data stored on TPA Firm systems. This information must be retained until legal, regulatory, and business requirements have been met.

Generally speaking, data may be retained for up to 120 days. However, data used for recurring transactions may be retained for as long as the customer's account remains with the TPA Firm. In the event that the customer's account is deleted, that customer's data must also be deleted/purged from all system components within 120 days using approved disposal methods.

Data Disposal

Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components.

Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps to

prevent such components from entering the gray market. The chosen method of disposal should be commensurate with the data sensitivity of the data being destroyed.

Methods for disposal include:

- Utilization of a secure wipe program for secure deletion (SDelete, Eraser, WipeFile, etc.)
- Crosscut shredding any data that is in hardcopy format

For electronic media stored on system components that are no longer in use, these system components must have data disposed of through any one of the following procedures:

- Disintegration
- Shredding (disk grinding device)
- Incineration by a licensed incinerator
- Pulverization

Customer data, whether in electronic media or hardcopy format, may reside in numerous places throughout the TPA Firm's environment. Below is a list of where customer data may be kept/stored:

Electronic Media

- Hard drives
- Tapes/media
- CDs/DVDs
- Compact flash drives, SD
- Dynamic Random Access Memory (DRAM)
- Read-Only Memory (ROM and the different variations thereof)

- Random Access Memory (RAM)
- Flash cards
- USB drives, removable media, memory sticks
- Databases
- Cloud-based resources
- Phone recordings

Hardcopy Format

- Plan documents or other supporting hardcopy documents and receipts
- Application printouts or other customer provided documentation
- Invoices
- Offline hardcopy batch printouts
- Other hardcopy formats as identified by TPA Firm

References

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Incident Response

Purpose

Incident response (IR) is a set of information security policies and procedures that you can use to identify, contain, and eliminate cyberattacks. The goal of incident response is to enable an organization to quickly detect and halt attacks, minimizing damage and preventing future attacks of the same type.

Employees share the responsibility of detecting and reporting security incidents. It is mandatory for all employees to assist the incident response procedures by managing their personal area of responsibility. The types of security incidents that an employee might likely encounter in their daily work routine includes:

- Security event notifications (e.g., natural disaster alerts, file integrity alerts, intrusion detection alarms, physical security alarms).
- Fraud, such as inaccurate database information or inaccurate logs/records.
- Theft or unauthorized access (e.g., surveillance/CCTV evidence of a break-in, missing items, unauthorized logins, broken locks).
- Unusual system behavior, such as unscheduled system reboots or abnormal errors in system log files/terminals).

Incident Response Components

The TPA Firm will document an Incident Response Plan that includes the following:

- How to recognize and report an incident
- Roles and responsibilities of incident response team members
- Defines reportable incidents
- Incident triage and criticality analysis
- Incident response reporting and communication requirements

- Incident containment
- Recovery and remediation
- Forensics
- Training for incident responders
- Lessons learned
- Provides metrics for measuring the incident response capability
- Testing of the plan
- Plan review/revision history

Responsiveness to Cybersecurity Incidents or Breaches

When a cybersecurity breach or incident occurs, appropriate action should be taken to protect the plan and its participants, including:

- Informing law enforcement
- Notifying the appropriate insurer
- Investigating the incident
- Giving affected plans and participants the information necessary to prevent/reduce injury
- Honoring any contractual or legal obligations with respect to the breach, including complying with agreed upon notification requirements
- Fixing the problems that caused the breach to prevent its recurrence

Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personally identifiable information or other sensitive data (i.e., breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

References

ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)

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

DE.AE-4: Impact of events is determined

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

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

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

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

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

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

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

RS.MI-1: Incidents are contained

RS.MI-2: Incidents are mitigated

RS.IM-1: Response plans incorporate lessons learned

RS.IM-2: Response strategies are updated

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Systems Operations

Purpose

An operations management system is a collection of processes and procedures that enables a company to effectively manage business practices and achieve the highest level of efficiency with day-to-day operations. Operations management systems are geared towards improving team performance and encouraging them to focus on tasks that are instrumental to their organization's growth.

Requirements

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency during system transition to operations and to maintaining the security support structure. System documentation and formalizing operational procedures with sufficient detail helps to eliminate security incidents and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that system operations will be performed correctly and efficiently.

- All phases of the systems lifecycle shall be formally documented.
- System owners shall formally document, approve and maintain detailed system and security operations and maintenance manuals/procedures for day-to-day and emergency IT operations.
- System Owners shall ensure that documentation is current, and personnel know where to find and how to reference them.
- Operational documentation containing sensitive information shall be assigned an appropriate security categorization and protected from unauthorized access and disclosure.
- Operations and maintenance documentation shall include, where applicable:
  - System and communications build/configuration specifications
  - Documented authorization from senior management to operate the system
  - System administration/maintenance manuals
  - Security Plans

- Security operations policy and procedures for:
  - Access Management
  - Data center security and safety
  - Incident Response and Handling
  - Baseline security configurations (OS, hardware/software, network, applications)
- Service Level Agreements
- Back-ups, storage and restore procedures
- Virus Update and Patch Management procedures
- Information, data, equipment and media handling, processing, and disposal procedures
- Business Continuity, Contingency, Disaster Response and Recovery plans
- Change Management procedures

References

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

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

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

PR.MA-2: Controlled Maintenance

PR.MA-6: Timely Maintenance

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

RS.AN-3: Forensics are performed

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Vulnerability and Patch Management

Purpose

Vulnerability management refers to the process of discovering, identifying, cataloging, remediating, and mitigating vulnerabilities found in software or hardware, while patch management refers to the process of identifying, testing, deploying, and verifying patches for operating systems and applications found on devices. By engaging in both vulnerability and patch management best practices, organizations can take a proactive approach to vulnerability remediation and mitigation. Patching vulnerabilities is a key element for cyber hygiene best practices and is a critical step in endpoint security.

Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure network, and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software.

Vulnerability Management

System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application services and ports are enabled and opened in the system's firewall, as applicable. Vulnerabilities that threaten the security of the TPA Firm's network or IT assets shall be addressed through updates and patches based upon assigned vulnerability ratings.

Vulnerability Identification

On a quarterly basis, or after any significant change in the network, the Information Security Department must conduct internal network vulnerability scans. Significant changes might include firewall rule modifications, product upgrades, system component installations or changes in network topography.

On an annual basis, or after any significant change to the network or after a significant application upgrade or modification, network and application layer penetration testing must be performed. A third-party IT security firm must perform all penetration testing unless approval is granted by senior management to allow a qualified internal resource with organizational independence to perform the penetration testing. Network layer penetration tests must include all components that support network functions and operating systems. In addition, testing must include internally and externally accessible IP addresses. Application layer penetration tests must be performed internally and externally. At a minimum, testing must consider the top 10 OWASP vulnerabilities.

If vulnerability scans or penetration tests uncover potential vulnerabilities, the appropriate personnel must be notified so remediation efforts may begin. Personnel must follow the Change Control Policy to correct high-level vulnerabilities. Additional scans or testing must then be performed in order to confirm compliance with the TPA Firm's security standards. In the event that the vulnerability cannot be remediated or mitigated, personnel must document the reason why it cannot, and proceed accordingly with any other compensating control.

In addition to vulnerability scanning and penetration testing, TPA security personnel must monitor common industry vulnerability news groups and security bulletins for vulnerabilities and potential workarounds that may not yet be known or resolved by the vendor.

Risk Ranking

Once a vulnerability is identified, the risk that vulnerability poses must be evaluated and ranked. This will allow the Information Security department to address high priority risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited. The NIST National Vulnerability Database provides a tool for calculating the Common Vulnerability Score for vulnerabilities that were not assigned a CVSS base score by the applicable vendor.

Patch Management

Failure to keep system components and other IT resources patched securely and on a consistent basis can cause unwanted damage to all environments directly associated with the systems and networks. Mitigation is a preventative control where patches are applied or new security controls are put in place to minimize the potential impact of a security event if a vulnerability is exploited. Remediation is the implementation of more complete security controls to eradicate the risk of a vulnerability being exploited. Often, mitigation is required while appropriate remediation activities are determined.

Mitigation timeframes for identified or assessed vulnerabilities shall be based on the assigned Vulnerability Risk Ranking:

- **Critical-level** risk vulnerabilities must be mitigated as soon as possible. “Critical-level risk” vulnerabilities must be, at a minimum, mitigated within 14 days, and remediated (if possible) within 28 days
- **High-level** risk vulnerabilities must be mitigated or remediated within thirty (45) days
- **Medium-level** risk vulnerabilities must be mitigated or remediated within sixty (75) days
- **Low-level** risk vulnerabilities must be mitigated or remediated within ninety (105) days

Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the When a vendor releases security updates, zero-day patches, and/or service packs, it is the Information Security Department’s responsibility to apply the changes as needed. The timeframe for installation on applicable systems is 30 days from the date of release, and the change management process must be followed. Automated patch management tools to facilitate flaw remediation must be used whenever possible to ensure the timeliness and completeness of system patching operations.

References

DE.CM-8: Vulnerability scans are performed

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

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

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)

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

System, Application, and Network Security

Purpose

A network monitoring application examines and tracks network activity for problems caused by malfunctioning hardware or overloaded resources such as firewalls, servers, routers, and network connections.

Continuous Monitoring Strategy

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base. Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

- Establishing and documenting the system-level metrics to be monitored
- Establishing and documenting the frequency for monitoring and frequency] for assessment of control effectiveness
- Ongoing control assessments in accordance with the continuous monitoring strategy
- Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy
- Correlation and analysis of information generated by control assessments and monitoring
- Response actions to address results of the analysis of control assessment and monitoring information
- Reporting the security and privacy status of the system to TPA Firm management

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs.

Malicious Code Protection Software

Systems that are commonly affected by malicious software must have an antivirus solution deployed and must include following:

- Be capable of detecting, removing, and protecting against all known types of malicious software
- Be configured to perform automatic updates
- Be configured to perform period scans
- Cannot be disabled by the employee
- Antivirus software log generation must be enabled, and antivirus logs must be retained for a minimum of 1 year

In addition, monitor the system to detect:

- Attacks and indicators of potential attacks in accordance with established monitoring objectives
- Unauthorized local, network, and remote connections

Identify unauthorized use of the system through the following techniques and methods:

- Invoke internal monitoring capabilities or deploy monitoring devices
- Analyze detected events and anomalies
- Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, or other organizations
- Obtain legal opinion regarding system monitoring activities
- Provide monitoring information to designated personnel as needed

System security professionals should investigate systems which currently do not require antivirus software for applicability and vendor notifications for such vulnerabilities.

Independent Security Control Assessments

A reliable third-party assessment of security controls provides a clear, unbiased report of existing risks, vulnerabilities, and weaknesses and must be conducted annually. An effective assessment program would include:

- Assessment reports, audit files, penetration test reports and supporting documents, and any other analyses or review of the TPA Firm's cybersecurity practices by an independent, third-party.
- Assessments and assessment reports prepared and conducted in accordance with appropriate standards.
- Documented corrections of any weaknesses identified in the independent third-party analyses.

References

PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)

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

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools

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

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

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

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

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

DE.AE-5: Incident alert thresholds are established

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

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

DE.CM-4: Malicious code is detected

DE.CM-5: Unauthorized mobile code is detected

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

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

DE.DP-3: Detection processes are tested

DE.DP-4: Event detection information is communicated

DE.DP-5: Detection processes are continuously improved

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Systems and Application Development and Performance

Purpose

A systems development methodology is a formalized, standardized, documented set of activities used to manage a system's development project. It should be used when information systems are developed, acquired, or maintained. Application development is the process of creating a computer program or a set of programs to perform the different tasks that a business requires. From calculating monthly expenses to scheduling sales reports, applications help businesses automate processes and increase efficiency.

Secure System Development Life Cycle Program (SDLC).

A secure SDLC process ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort. Best practices include:

- Procedures, guidelines, and standards which ensure any in-house applications are developed securely. This would include such protections as:
  - Configuring system alerts to trigger when an individual's account information has been changed.
  - Requiring additional validation if personal information has been changed prior to request for a distribution from the plan account.
  - Requiring additional validation for distributions (other than a rollover) of the entire balance of the participant's account.
- Procedures for evaluating or testing the security of externally developed applications including periodic reviews and updates.
- A vulnerability management plan, including regular vulnerability scans.
- Annual penetration tests, particularly with respect to customer-facing applications.

Performance Security

The principle of performance security states that security mechanisms are constructed so that they do not degrade system performance unnecessarily. Stakeholder and system design requirements for performance and security are precisely articulated and prioritized.

For the system implementation to meet its design requirements and be found acceptable to stakeholders (i.e., validation against stakeholder requirements), the designers adhere to the specified constraints that capability performance needs place on protection needs. The overall impact of computationally intensive security services (e.g., cryptography) are assessed and demonstrated to pose no significant impact to higher-priority performance considerations or are deemed to provide an acceptable trade-off of performance for trustworthy protection.

The trade-off considerations include less computationally intensive security services unless they are unavailable or insufficient. The insufficiency of a security service is determined by functional capability and strength of mechanism. The strength of mechanism is selected with respect to security requirements, performance-critical overhead issues (e.g., cryptographic key management), and an assessment of the capability of the threat.

The principle of performance security leads to the incorporation of features that help in the enforcement of security policy but incur minimum overhead, such as low-level hardware mechanisms upon which higher-level services can be built. Such low-level mechanisms are usually very specific, have very limited functionality, and are optimized for performance. For example, once access rights to a portion of memory is granted, many systems use hardware mechanisms to ensure that all further accesses involve the correct memory address and access mode. Application of this principle reinforces the need to design security into the system from the ground up and to incorporate simple mechanisms at the lower layers that can be used as building blocks for higher-level mechanisms.

Secure Application Development

Establish and maintain a secure application development process. In the process, address such items as:

- Secure application design standards
- Secure coding practices
- Developer training
- Vulnerability management
- Security of third-party code
- Application security testing procedures

Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

References

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

PR.AC-3: Remote access is managed

PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Physical Security and Environmental Controls

Purpose

Physical and environmental security programs define the various measures or controls that protect organizations from loss of connectivity and availability of computer processing caused by theft, fire, flood, intentional destruction, unintentional damage, mechanical equipment failure, and power failures. Physical security measures should be sufficient to deal with foreseeable threats and should be tested periodically for their effectiveness and functionality.

Physical Security

Physical security controls include physical access control devices (such as badges or keys), physical intrusion and detection alarms, operating procedures for facility security guards, physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas, and monitoring or surveillance equipment. Physical access controls apply to employees and visitors.

- Enforce physical access authorizations at entry and exit points to the facility where the system resides by:
  - Verifying individual access authorizations before granting access to the facility
  - Controlling ingress and egress to the facility using one or more physical security controls such as security guards, badges, or lock and key
- Maintain physical access audit logs for entry and exit points to the facility
- Control access to areas within the facility designated as publicly accessible by implementing the following controls:
  - Escort visitors and control visitor activity
  - Secure keys, combinations, and other physical access devices
  - Inventory physical access devices every quarter
  - Change combinations and keys when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to facilities and systems. Physical access to the facility where the system resides must be monitored to detect and respond to physical security incidents:

- Review physical access logs daily and upon occurrence of unusual or suspicious activity, anomalous events, or potential threats
- Coordinate results of reviews and investigations with the organizational incident response capability
- Provide designated personnel with initial and annual training in the employment and operation of physical security controls.

Physical access monitoring includes publicly accessible areas within the TPA Firm's facilities. Examples of physical access monitoring include the employment of guards, video surveillance equipment (i.e., cameras), and sensor devices. The log reviews can be supported by audit logging controls if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Environmental Controls

Emergency Shutoff

IT Department shall:

- Provide the capability of shutting off power to the information system or individual system components in emergency situations.
- Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorized activation.

Emergency Power

IT Department shall:

- Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system, transition of the information system to long-term alternate power in the event of a primary power source loss.
- Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Emergency Lighting

IT Department shall:

- Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
- Provide emergency lighting for all areas within the facility supporting essential missions and business functions.

Fire Protection

IT Department shall:

- Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

  This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Temperature and Humidity Controls

IT Department shall:

- Maintain temperature and humidity levels within the facility where the information system resides at [entity defined acceptable levels].
- Monitor temperature and humidity levels [entity defined frequency] to include alarms or notifications of changes potentially harmful to personnel or equipment.

Water Damage Protection

IT Department shall:

- Protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

  This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

References

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

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

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

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

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

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

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Vendor and Third-Party Service Provider Management

Purpose

Service providers are outsourced third-party organizations that manages some aspect of day-to-day operations. These organizations provide services that take on tasks essential to the success of businesses, but rarely interact with clients. Vendors can be anyone from a business' furniture supplier or cleaning services to their Internet provider. The management of these relationships is crucial for businesses.

The TPA Firm must make every effort to assure all third-party organizations are compliant and do not compromise the integrity, security, and privacy of the Firm's or its customer's data. Third parties include customers, partners, subcontractors, and contracted developers.

Due Diligence

An inventory of third-party service providers shall be maintained. Critical providers must be identified, and an annual risk assessment must be conducted for all critical providers. The service provider inventory will include:

- Vendor risk level
- Types of data shared with the third-party
- Brief description of services
- Main point of contact at the third-party
- How access is granted to the third-party vendor (logical and/or physical)
- Significant controls in place
- Security policy/report and/or questionnaire

IT vendors are prohibited from accessing the TPA Firm's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.

- All IT vendors must comply with the security policies defined and derived from the TPA Firm's Information Security Program

to include the Acceptable Use Policy.

- IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. The Firm strictly adheres to all applicable legal, regulatory, and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally Identifiable Information (PII).

The TPA Firm may choose to assess IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.

Considerations for Software Vendors

Only use up-to-date and trusted third-party components for the software developed by the organization. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

Establish and manage an updated inventory of third-party components used in development, often referred to as a “bill of materials,” as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components and validate that the component is still supported.

Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization’s authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.

Vendor Contracts, Online Terms, and Policies

Formal contracts or online terms and policies that address relevant security and privacy requirements must be in place for all third parties that process, store, or transmit confidential data or provide critical services. Management approval is required before contracting with cloud-hosted solutions or off-site hosting services and must ensure vendor compliance with appropriate security policies. TPA Firm shall ensure that contract language requires vendors to provide as attestation to their compliance, an industry recognized, third-party assessment report.

The following must be included in all such contracts (or online terms and policies):

- Contracts will acknowledge that the third-party is responsible for the security of the TPA Firm's confidential data that it possesses, stores, processes, or transmits
- Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party
- Contracts identify information security policies relevant to the agreement
- Contracts establish training and awareness requirements for specific procedures and information security requirements
- Contracts identify relevant regulations for sub-contracting
- Contracts implement a monitoring process and acceptable methods for validating the adherence to security requirements of delivered information and communication technology products and services
- Contracts implement specific processes for managing information and communication technology component lifecycle and availability and associated security risks
- Contracts identify and outline use of key controls to ensure the protection of organizational assets – e.g., controls for protection against malicious code, physical protection controls, controls to protect integrity, availability and confidentiality of information, controls to ensure the return or destruction of information assets after their use, controls to prevent copying and distributing of information
- Contracts define information security requirements and identify the owner of information and how intellectual property rights are regulated
- Contracts identify the recourse available to the TPA Firm should the third-party fail to meet defined security requirements
- Contracts establish responsibilities for responding to direct and indirect security incidents including timing as defined by service-level agreements (SLAs)
- Contracts specify the security requirements for the return or destruction of data upon contract termination
- Contracts stipulate geographic limits on where data can be stored or transmitted
- Contracts specify responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties
- Contracts require, in addition to initial validation, cloud/vendor must annually provide validation of their continued compliance to applicable frameworks and standards. This requirement includes all vendors supporting Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and/or Software as a Service (SaaS).
    - Examples of acceptable assessment reports include, Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, SSAE 16, and ISO 27001.
    - Cloud Service Providers (CSPs) must demonstrate that continuous monitoring activities are in place and compliance is being met.

Vendor Services Change Management

Changes to the provision of services by vendors, including maintaining and improving existing information security policies, procedures, and controls, should be managed, taking account of business information criticality, systems and processes involved, and re-assessment of risks. The following aspects will be considered:

- Changes to supplier agreements
- Changes made by the organization to implement
- Enhancements to the current services offered
- Development of any new applications and systems
- Modifications or updates of the organization's policies and procedures
- New/changed controls to resolve security incidents and improve security

Changes in supplier services to implement:

- Changes and enhancement to networks
- Use of new technologies
- Adoption of new products or newer versions/releases
- New development tools and environments
- Changes to physical location of service facilities
- Change of suppliers
- Subcontracting to another supplier

Vendor Risk Assessment

Vendor Risk Management (VRM) is the process of managing risks associated with third-party vendors. It's important to understand these risks, what they are, and how the TPA Firm can readily identify any issues, concerns, or constraints pertaining to these risks. Failure to mitigate and prevent these risks can result in significant financial loss, reputational damage, and/or legal/regulatory issues. As such, the following risks are to be thoroughly understood and assessed in regard to business and contractual relationships entered into with vendors:

- **Strategic Risk**: Risk of failing to implement or achieve planned business goals, objectives, or initiatives. Inability to address the fundamentals required to execute the agreed strategy, as evidenced by deviations from business plans.
- **Compliance Risk**: Risks arising from violations of applicable laws, rules, regulatory mandates, and along with other issues, such as non-compliance of operational, and information security policies, procedures, and processes.
- **Operational Risk**: Risks from a failed system of operational internal controls relating to relevant policies, procedures, and practices. Specifically, failures associated with processes, systems, or people.
- **Financial Risk**: Risks related to the financial condition of the third-party vendors, such as a vendor under the threat of liquidation in the foreseeable future.
- **Reputation Risk**: Risks of negative public perception and opinion, such as unethical business practices or data breaches resulting in loss of sensitive and confidential consumer information.
- **Technology Risk**: Risks from any number of information technology and information governance and security issues, including inadequate resources (hardware, software, or manpower).
- **Country Risk**: Risks arising from the political, economic, and social landscape and other relevant events within a foreign country that can impact the services provided by vendors, ultimately affecting company operations.
- **Environmental, Social and Governance Risk**: Risks related to climate change impacts, environmental practices, and duty of care, working and safety condition, respect for human rights, and compliance with laws and regulations.

Vendor risk level assessments will be based on the following considerations:

- **High**: the vendor stores or has access to sensitive data and a failure of this vendor would have critical impact on the Firm's business
- **Moderate**: the vendor does not store or have access to sensitive data and a failure of this vendor would not have critical impact on the Firm's business
- **Low**: the vendor does not store or have access to any data and a failure of this vendor would have very little to no impact on the Firm's business

References

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

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

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

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.

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.

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Cybersecurity Awareness Training

Purpose

Employees are often an organization's weakest link for cybersecurity. A comprehensive cybersecurity security awareness program sets clear cybersecurity expectations for all employees and educates everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat.

A security awareness training program shall be established for all contractors, third-party users, and employees of the TPA Firm and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in Firm procedures, processes, and policies relating to their professional function relative to the Firm.

The TPA Firm provides basic and advanced levels of awareness training to system users, including measures to test the knowledge level of users. The TPA Firm determines the content of awareness training based on specific Firm requirements, the systems to which personnel have authorized access, and work environments (e.g., work from home).

Since identity theft is a leading cause of fraudulent distributions, it should be considered a key topic of training, which should focus on current trends to exploit unauthorized access to systems. Be on the lookout for individuals falsely posing as authorized plan officials, fiduciaries, participants, or beneficiaries.

The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Security awareness training is to be provided as part of the initial training for new users and annually thereafter or when required by system changes. Training content will be updated at least annually and will incorporate lessons learned from internal and external security incidents.

Multiple methods of delivery will be employed to increase the security of system users. Awareness techniques can include:

- Displaying posters
- Offering supplies inscribed with security reminders
- Displaying logon screen messages
- Generating email advisories or notices from TPA Firm officials
- Hosting security awareness events

References

ID.GV-1: Organizational cybersecurity policy is established and communicated

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.

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.

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

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Encryption in Transit and at Rest

Purpose

Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. Data protection in transit is the protection of data while it travels from network to network or is transferred from a local storage device to a cloud storage device. Wherever data is moving, effective data protection measures for in transit data are critical as data is often considered less secure while in motion.

Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network. While data at rest is sometimes considered to be less vulnerable than data in transit, attackers often find data at rest a more valuable target than data in motion. The risk profile for data in transit or data at rest depends on the security measures that are in place to secure data in either state.

Encryption Key Management

Encryption keys must be generated, accessed, and stored in a secure manner.

In order to generate a strong key, a random or pseudo-random number generation algorithm must be used. The minimum length requirements for the encryption keys are 128 bits. Examples of acceptable algorithms are as follows:

- AES: 128 bits
- RSA: 2408 bits
- Follow vendor recommendations for other encryption types.

TPA Firm must maintain a documented description of the cryptographic architecture that includes:

- Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date

- Description of the key usage for each key
- Inventory of any HSMs and other SCDs used for key management

TPA Firm attests that the following steps are being taken to protect encryption keys against disclosure and misuse:

- Access to keys is restricted to the fewest number of custodians necessary
- Key-encrypting keys are at least as strong as the data-encrypting keys they protect
- Key-encrypting keys are stored separately from data-encrypting keys
- Keys are stored securely in the fewest possible locations and forms
- Any key used to either encrypt or decrypt cardholder data must be stored separately from general user access. Note: Key components may only be accessed by authorized key custodians.

At least two key custodians must be authorized in order to successfully perform a key action, such as key generation or loading the key. No individual key supervisor may have access to all pieces of a data encryption key. Each custodian will generate one text piece used in the key generation. Any type of access to the key generating procedures must be limited to authorized custodians and kept secure to prevent unauthorized key generation or replacement.

Encryption key component access will only be given to key custodians with a job duty that requires access. TPA Firm management, or their designee, will be responsible for granting access by utilizing an ‘Authorization Request Form’. Users who have been granted access must complete and sign an ‘Encryption Key Custodianship Form’. By signing the form, the user recognizes their responsibilities as a key custodian. Human Resources will maintain a copy of this form in the user’s employee records.

Only those authorized key custodians will be allowed to retrieve the key components from their secure location and distribute keys. Key custodians must track and log their activities within an ‘Encryption Key Management Log’. Before being returned to secure storage, the custodian must place the encryption keys in secure packaging.

During an encryption key change process, the key custodian generates a new key, decrypts the current production data, and re-encrypts the sensitive data with the new encryption key.

On an annual basis, or whenever conditions warrant a change in key integrity, the encryption keys must be changed. Conditions for a key change include:

- Annual Rotation: Keys are to be changed once per year (minimum)
- Suspicious Activity: Keys are to be changed if any activity related to the key process raises concern or is otherwise deemed suspicious
- Resource Change: Keys are to be changed if a key supervisor's employment ends or a key custodian accepts a position within the TPA Firm that does not involve the key encryption process
- Technical Requirement: Keys are to be changed if a technical issue arises that questions the durability or security of a key (corruption or instability)

In order to dispose of an unwanted encryption key, key custodians must follow approved Firm methods for secure data disposal.

Encryption of Sensitive Data Stored and in Transit

Data encryption can protect nonpublic information. A system should implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data at rest or in transit.

Employ encryption to protect the confidentiality and integrity of information on managed mobile devices.

Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

References

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

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

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Remote Work

Purpose

Remote work is a type of flexible working arrangement that allows an employee to work from remote location outside of corporate offices. For employees who can complete work offsite, this arrangement can help ensure work-life balance, access to career opportunities or reduced commutation costs. Benefits for the company include increased employee satisfaction and retention, increased productivity, and cost savings on physical resources. Remote work arrangements can be temporary or permanent, part-time, or full-time, occasional, or frequent. Remote work requires policies governing equipment use, network security and performance expectations.

An employee may be eligible to work remotely if their duties can be met through basic hardware and software standards, they have proven to be trustworthy, disciplined, and self-motivated, and have been given permission by the TPA Firm.

Employees must follow the work schedules provided to them, continue to meet objectives and deadlines, uphold high-quality standards, and submit reports as required by the employee's manager. While some flexibility is allowed, the employee's work schedule, total work hours, scheduled workdays, and times of availability are subject to a review between the employee and their resource manager and may be adjusted to meet changes in client or industry demands.

Tools and instructions will be made available to employees for managing time and tasks, communicating with co-workers, logging and tracking projects, and accessing resources.

Performance will be measured, focusing on the same metrics that apply to work done in the office.

Communication

Employees are to be online and accessible for the duration of their assigned work shift as agreed upon by their resource manager. They are expected to check-in with their managers at least once a day.

Any correspondence from a co-worker or client must be answered as quickly as possible.

Tools such as instant messaging, e-mail, VoIP, and conferencing solutions have been provided for communicating with team members and clients for project collaboration.

Resource meetings will be scheduled for at least once a week. Times are to be discussed and agreed upon between the employee and manager.

Security

An inventory should be maintained by the TPA Firm of all remote end-point devices used by employees. The inventory should include the make/model of the device as well as the operating system, programs/data, and version installed on the device.

When not in use, all company equipment should be powered off and stored in a secure location to prevent accidental or intentional misuse.

System Settings

- Employees will be given access to a Virtual Private Network to securely connect to company servers and networks
  - The VPN must be used at all times during work hours
  - Multi-factor authentication must be enabled for the VPN connection
  - All VPN connections will timeout and force reauthentication after four hours of continuous connection
- Personal firewall must be installed and actively running
  - The employees must not be able to alter their personal firewall settings
- Systems that are commonly affected by malicious software must have an antivirus solution deployed and must include following:
  - Be capable of detecting, removing, and protecting against all known types of malicious software
  - Be configured to perform automatic updates
  - Be configured to perform period scans
  - Cannot be disabled by the employee
  - Antivirus software log generation must be enabled, and antivirus logs must be retained for a minimum of 1 year

- Remote endpoints should be configured so that only necessary services, protocols, etc. are enabled
    - All vendor-supplied default accounts should be removed or disabled, and default passwords must be changed
- Remote endpoints must be updated with the latest critical security patches prior to deployment to the employee and kept current by the employee as instructed by members of the IT department
- Configuration changes made to remote endpoints must be approved and follow the company's change control process
- Employees must be assigned a unique user ID and a strong password for access to systems
    - Generic and shared accounts may not be used
- Multi-factor authentication must be used for all remote access to the corporate network

References

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Roles and Responsibilities

Purpose

Roles are required within the organization to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished. Their purpose is to clarify, coordinate activity, and actions necessary to disseminate security policy, standards, and implementation.

For a cybersecurity program to be effective, it must be managed at the senior executive level and executed by qualified personnel.

Chief Information Security Officer (CISO)

As a senior executive, the Chief Information Security Officer (CISO) would generally establish and maintain the vision, strategy, and operation of the cybersecurity program which is performed by qualified personnel who should meet the following criteria:

- Sufficient experience and necessary certifications.
- Initial and periodic background checks.
- Regular updates and training to address current cybersecurity risks.
- Current knowledge of changing cybersecurity threats and countermeasures.

System Security Personnel, Employees, Contractors, and Third Parties

Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable.

Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.

Roles and responsibilities must be reviewed annually, or when significant enterprise changes occur that could impact this Safeguard.

References

PR.AT-2: Privileged users understand their roles and responsibilities

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

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

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

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

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

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

PR.AT-4: Senior executives understand their roles and responsibilities

PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Sanctions

Purpose

Sanctions, or disciplinary actions, are designed to set and maintain standards of conduct within the Firm, and in doing so, ensure that all employees are treated fairly and consistently. They are designed to help and encourage all employees to achieve and maintain satisfactory standards of conduct.

Employees are expected to meet performance standards and conduct themselves appropriately. This policy is intended to provide tools for addressing employee conduct and performance issues in a reasonable, consistent, and effective manner.
Any disciplinary action issued in accordance with this policy must be for just cause under one or more of the three following reasons:

- Unsatisfactory job performance
- Unacceptable personal conduct
- Grossly inefficient job performance

Anyone found in violation of these policies will be subject to disciplinary action up to and including termination. TPA Firm management will determine how serious an employee's offense is and take the appropriate action.

References

US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Informative References

Policy	Informative References
Data Governance and Classification	• CIS CSC 13, 14 • COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
Data Privacy	• CIS CSC 1, 5, 15, 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 • CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15 • CIS CSC, 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

Access Controls and Identity Management	• CIS CSC 1, 5, 15, 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 • CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15 • CIS CSC, 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
Business Continuity and Disaster Recovery	• CIS CSC 19 • COBIT 5 APO12.06, DSS04.03 • ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 • NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP13, IR-7, IR-8, IR-9, PE-17 • CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 • COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • COBIT 5 MEA03.02 ISO/IEC 27001:2013 Clause 7.4

	• COBIT 5 MEA03.02 ISO/IEC 27001:2013 Clause 7.4 • COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4
Configuration Management	• COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 • CIS CSC 3, 11 COBIT 5 BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 • CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7
Asset Management	• CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5 • CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5 • CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 • CIS CSC 12 1. COBIT 5 APO02.02, APO10.04, DSS01.02 2. ISO/IEC 27001:2013 A.11.2.6 3. NIST SP 800-53 Rev. 4 AC-20, SA-9 • CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST

	SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6 • CIS CSC 10 COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
Risk Assessment	• CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16 • CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM16 • CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM9, PM-11 • CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 • CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9 • COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 ISO/IEC 27001:2013 Clause 6 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM9, PM-10, PM-11 • CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9 • • COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9 • COBIT 5 APO12.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST

	SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM11 • • CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
Data Retention and Disposal	• COBIT 5 BAI09.03, DSS05.06 ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 NIST SP 800-53 Rev. 4 MP-6 • CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
Incident Response	• COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA14 • CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14 • CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4 • CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 • CIS CSC 19 COBIT 5 DSS01.03 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 • CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 • CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • CIS CSC 19 COBIT 5 BAI08.04 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-

	53 Rev. 4 SI-5, PM-15 • COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4 • CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 • CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4 • CIS CSC 4, 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4 • COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
Systems Operations	• COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14 • CIS CSC 18, 20 COBIT 5 BAI03.08, BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2 • CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03 ISA 62443-2-1:2009 4.3.4.3.3 ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI13, SI-14, SI-16, SI-17 • COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ISA 62443-2-1:2009 4.3.2.5.2 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP13, PL-8, SA-14, SC-6 • COBIT 5 APO12.06, DSS03.02, DSS05.07 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4

Vulnerability and Patch Management	• CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5 • CIS CSC 4 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 • CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 • CIS CSC 4, 19 COBIT 5 EDM03.02, DSS05.07 NIST SP 800-53 Rev. 4 SI-5, PM-15
System, Application, and Network Security	• COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8 • CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7 • CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7 • COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6 • CIS CSC 8, 12, 15 COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC38, SC-39, SC-40, SC-41, SC-43 • CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4

	• CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 • CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 • CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM3, SC-5, SC-7, SI-4 • CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 • CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8 • CIS CSC 7, 8 COBIT 5 DSS05.01 ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44 • CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 • COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA18, SI-4, PM-14 • COBIT 5 APO13.02, DSS05.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14 • CIS CSC 19 COBIT 5 APO08.04, APO12.06, DSS02.05 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA5, SI-4 • COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA5, SI-4, PM-14 • CIS CSC 4, 6, 8, 19 COBIT 5 DSS02.04, DSS02.07 ISA 62443-2-1:2009

	4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
Systems and Application Development and Performance	• COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8 • CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10 • CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family • CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 • CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
Physical Security and Environmental Controls	• COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 • COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE14, PE-15, PE-18 • COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6,

	PE-20 • COBIT 5 BAI03.05 ISA 62443-2-1:2009 4.3.4.4.4 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7 • CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, DSS05.06 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP5, MP-7, MP-8 • COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 • COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
Vendor and Third-Party Service Provider Management	• COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA14, SA-15, PM-9 • COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12 • CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2 • COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM9 • COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU16, PS-7, SA-9, SA-12

	• CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9 • CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
Cybersecurity Awareness Training	• CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls from all security control families • CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13 • CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 • CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 4 -1 controls from all security control families
Remote Work	• US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices
Encryption In Transit and At Rest	• US Department of Labor, Employee Benefits Security Administration, Cybersecurity Program Best Practices

Roles and Responsibilities	• CIS CSC 5, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13 • CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC5, AC-6, AC-14, AC-16, AC-24 • CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 • COBIT 5 BAI08.04, DSS03.04 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 • CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 • CIS CSC 19 COBIT 5 EDM03.02, APO01.02, APO12.03 ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8 • CIS CSC 17, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13 • CIS CSC 17 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13

Glossary

Term	Definition
Confidential Information	Information that is not Restricted but must be protected from unauthorized access, modification and/or destruction because it has a high risk of causing reputational or other harm to the TPA Firm if not properly protected.
Data Administrator	Works with the data stewards to establish procedures for the responsible management of data, including data entry and reporting.
Data Steward	Authorizes the use of data within their functional areas and monitors this use to verify appropriate data access.
Encryption	A form of data security in which information is converted to ciphertext. Only authorized people who have the key can decipher the code and access the original plaintext information. In even simpler terms, encryption is a way to render data unreadable to an unauthorized party.
Executive Sponsor	The senior manager responsible and accountable for major administrative data systems within their functional area.
Internal Information	Information that does not rise to the level of Confidential but is not intended for public use.
Mitigation	Implementing temporary solutions to lesson the likelihood of a security vulnerability being exploited.
Multi-Factor Authentication	An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence
Public Information	Information that may be freely shared with the public.
Remediation	The process of recognizing vulnerabilities and threats and taking the necessary actions to eliminate them.

Restricted Information	Information that must be protected from unauthorized access, modification and/or destruction in accordance with regulation, law, and/or company policy.
Segmentation	A network security technique that divides a network into smaller, distinct sub-networks that enables network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network.
Sensitive Data	Information sensitivity is the control of access to information or knowledge that might result in loss of an advantage or level of security if disclosed to others