CompTIA

WORKBOOK

cybersecurity standard

This Workbook is designed to help you understand and implement the recommended best practices defined by the CompTIA Channel Standard for Cybersecurity. It includes the best practice, questions to consider to determine how well that practice is in place, and some recommendations on how to address the best practice.

The Standard is based on the NIST Cybersecurity Framework and interpreted to be meaningful for IT Solution Providers. The Standard and Workbook together define the intelligent business practices integral to building a sound security posture for your organization and your clients. To demonstrate adherence to the Standard, consider earning the CompTIA Security Trustmark+. The Trustmark+ program uses the same Channel Standard for Cybersecurity and includes a 3rd party assessment of your documentation, policies, and procedures to show the due diligence undertaken by the applying organization.

Though this Standard represents the input of numerous experts over countless hours of experience and meeting with IT businesses to learn about them; the outcome will be dependent on execution and a number of market-specific as well as economic factors beyond the scope of this standard.

Only with honest self-reflection can a business effectively evaluate itself against this checklist. Throughout that process, the company and its management team can embrace incremental improvements; focus on establishing and meeting the ever-increasing expectations of their clients; in addition to creating a highly professional environment for employees.

The CompTIA Channel Standard for Cybersecurity provides intelligent business practices for the five pillars of IT security and has been categorized along those lines. By reviewing the Standard and comparing to reality, a full picture of functional best practices for your business is created. These are the five pillars of IT security:

- Identify
- Protect
- Detect
- Respond
- Recover

Furthermore, each of the 5 categories are further broken down into functional areas to help group related practices together.

Given the amount of content contained within this Workbook, a roll-up of the recommended documents that make up an IT Security Policy is listed here. These plans and documents may help you implement the best practices suggested within this standard.

Recommended Document	Purpose
IT Security Policy & Procedures	Overall document containing the various plans and procedures related to IT Security.
Risk Assessment	An evaluation of the potential risks and threats to the organization, based on their business purpose and role in the industry.
Business Impact Analysis	An analysis reporting on the impact on the business of a variety of recognized threats.
Incident Response Plan	A plan defining the roles, procedures, and expectations in the case of a security incident.
Business Continuity Plan	A plan addressing how a business will stay up and running in the case of any service interruption.
Disaster Recovery Plan	A plan specifically addressing major disaster recoveries, as opposed to regular incidents.
Hardware Inventory	List of hardware assets.
Network Diagram	Diagram of the network, connections, and ports.
Service Provider List	List of contracted service providers.
Data Classification Policy	Defines how data is classified.
Job Description	Employee job descriptions.
Regulatory Compliance	In the case of regulatory needs, an approval document from the regulating body.
Training History	Technical, expert, and general security awareness training records for all employees.
Protection Communication	Communication plan to address protections.

In some cases, you may find cross-over between documents. You may also find you have fewer documents or differently named documents. As long as the content in the document supports the related best practice, the specific name or location of a document may be different than what the chart recommends.

Category 1

Identify

When thinking about a system of security, it's recommended to first get a handle on the scope of assets, individual roles, and the governing policies to manage the system.

The IDENTIFY section provides the functional areas that should be reviewed, recorded, and regularly updated to maintain an understanding of the policy guidance, assets, roles, partners, and risks inherent managing the business. It also addresses planning for Security and Vulnerability Management Programs and utilizing a Risk Management Framework.

Identify has been broken down into 3 sub-categories: **Inventory**, **Roles & Interdependencies**, and **Governance**.

IDENTIFY: INVENTORY

HARDWARE MANAGEMENT – Maintain accurate inventories of information systems and devices.

Identifying and prioritizing information assets according to criticality is essential for a business to properly manage risk, so that protections can be applied commensurate with the assets importance. Information systems and devices refer to any piece of hardware (desktop, laptop, mobile phone, tablet, server, etc.) considered property of the organization. Reports should be maintained in either manual or automated systems.

Questions to consider internally:

Questions to consider internally:

Do you maintain accurate inventories of hardware?

Where are these inventories maintained, and how can they be accessed/updated?

Recommendations:

Be able to demonstrate that a current and comprehensive baseline inventory exists that includes manufacturer, type, model, and physical location. If required to share this information, the report should be available in any variety of ways, such as: screen capture, .csv file, export from excel file, word document, spreadsheet, etc.

Don't forget to take notes!

IDENTIFY: INVENTORY

SOFTWARE MANAGEMENT – Maintain accurate inventories of its approved software and applications.

Identifying and prioritizing software according to criticality is essential for a business to properly manage risk, so that protections can be applied commensurate with the assets importance. Approach software management similarly to hardware management.

Questions to consider internally:

Do you maintain an accurate inventory of software and applications?

Where are these inventories maintained, and how can they be accessed/updated?

Recommendations:

Be able to demonstrate that a current and comprehensive baseline inventory exists of all software that includes manufacturer, type, and version. If required to share this information, the report should be available in any variety of ways, such as: screen capture, .csv file, export from excel file, word document, spreadsheet, etc.

Don't forget to take notes!

IDENTIFY: INVENTORY

DATA FLOW MANAGEMENT – Manage and document data flow management.

Without documenting the data that is legitimately supposed to flow across the network (e.g., ports, protocols, and services), it is not possible to implement least functionality precautions or even know what "bad" traffic is on the network.

Questions to consider internally:

How do you document data flow management?

Recommendations:

Maintain a current and comprehensive network diagram that includes allowed ports, protocols and services. Be able to produce this documentation as required. Associated risks of not managing data flow include lapses in security coverage, unmitigated vulnerabilities, or non-compliance.

Don't forget to take notes!

IDENTIFY: INVENTORY

EXTERNAL INFORMATION SYSTEMS – Hosted or maintained services by 3rd parties are documented.

With the growing reliance on outsourced IT services, it is critical for businesses to understand where their data/services are hosted and what security precautions are in place to protect those critical services and data.

Questions to consider internally:

Do you document the systems and services hosted or maintained by 3rd parties?

How do you ensure the 3rd party is aware of this requirement?

Recommendations:

Maintain a current and comprehensive Service Provider vendor list to inventory all software and systems, including manufacturer, type, and version. Be able to produce this report as needed. Associated risks of failing to maintain records of 3rd party systems include regulatory non-compliance, poor network visibility, lapses in security coverage, and unmitigated vulnerabilities.

Don't forget to take notes!

IDENTIFY: INVENTORY

RESOURCE VALUE CATEGORIZATION – Assign a classification for all assets and resources.

To apply the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations, data, whether electronic or printed, must be classified. Consistent use of data classification reinforces with users the expected level of protection of data assets in accordance with required security policies.

Questions to consider internally:

Does a Data Classification Policy or Standard exist within the organization?

How do you classify data?

Are owners associated to data?

Recommendations:

Data classification provides a framework for managing data assets and information resources based on utility to the organization, intrinsic financial value and impact of loss and other associated risks. The data owner should consult with the Information Security organization and legal counsel on the classification of data as Restricted, Confidential, Agency-Internal, or Public. Documentation should be maintained that describes how assets and resources are classified, based on factors important to the organization.

Don't forget to take notes!

IDENTIFY: ROLES AND INTERDEPENDENCIES

IT SECURITY ROLES & RESPONSIBILITIES – User roles and responsibilities are established and documented.

It is important to know how roles work together to keep a company secure. Documenting these roles and responsibilities reduces assumptions and improves security awareness.

Questions to consider internally:

Do you establish IT Security user roles and responsibilities?

How are these roles identified, filled, and communicated?

Recommendations:

Document IT security roles and responsibilities. Evidence could be assignment orders or a general management statement of roles and responsibilities. Ensure that all responsibilities have been specifically assigned to an owner. Failure to identify and document security roles can lead to lack of accountability, ad-hoc response processes, and poor visibility into security precautions.

Don't forget to take notes!

SUPPLY CHAIN STAKEHOLDERS & INTERDEPENDENCIES –

Document stakeholder relationships within the supply chain.

Hackers have found that sometimes the easiest way to get into a network is through exploiting weaknesses in the supply chain. This involves ensuring that only reputable vendors and products are allowed to be used.

Questions to consider internally:

Do you document supply chain interdependencies among stakeholders?

How do you express security concerns to 3rd parties and validate their conformance to your security requirements?

Recommendations:

Document any formal or informal risk assessments of the organization's supply chains and that include reason why vendors are chosen. Conduct and document threat assessments for weaknesses in the supply chain. Documentation such as a summary of stakeholder relationships, Business Impact Analysis (BIA) that identifies those relationships, and/or a Risk Assessment (RA) can all help manage this concern.

Don't forget to take notes!

IDENTIFY: ROLES AND INTERDEPENDENCIES

BUSINESS ROLE – Recognize the organization's role within its industry is and identify applicable risk.

Certain businesses have wide-ranging impact on other industries. Understanding that business role and managing risk appropriately is important for businesses to take seriously.

Questions to consider internally:

Do you understand the role you play in identifying applicable risk for your customers?

Are you comfortable in the role you have been positioned?

Recommendations:

If applicable, a statement from management, mission statement or some other awareness of the critical role played by the organization should be drafted. If the business role begins to stray from what is comfortable or required, consider other ways to manage or remove the risk exposure.

Don't forget to take notes!

IDENTIFY: ROLES AND INTERDEPENDENCIES

MISSION, OBJECTIVES & ACTIVITIES – Ensure organizational awareness of critical business functions.

Without a clear understanding of mission and objectives for a business, this can have a negative, cascading effect on overall IT security preparation. This affects the ability to protect against, respond to, and recover from incidents.

Questions to consider internally:

How are the mission and objectives established and communicated to the organization?

Recommendations:

A mission, vision, objectives and strategy exist, have been documented, and is reviewed with business activities to ensure they support one another. This will also help solidify the roles employees play in achieving that mission.

Don't forget to take notes!

IDENTIFY: ROLES AND INTERDEPENDENCIES

DEPENDENCIES ANALYSIS – Document dependencies and functions for the delivery of critical services.

Without a clear understanding of how critical systems work and understanding dependencies, this can have a negative, cascading effect on overall IT security preparation. This affects the ability to protect against, respond to, and recover from incidents.

Questions to consider internally:

How do you identify and document functions and dependencies critical for the delivery of services?

How do you consider the impact of these dependencies on your ability to meet the service levels committed to clients?

Recommendations:

Maintain a summary of dependencies, Business Impact Analysis (BIA), or a Risk Assessment (RA) that describes the systems and processes that allow critical systems to operate.

Don't forget to take notes!

IDENTIFY: ROLES AND INTERDEPENDENCIES

RESILIENCY ANALYSIS – Document resilience requirements to support the delivery of critical services.

Understanding the criticality of systems will help identify what the acceptable levels of downtime are and what controls can be put in place to ensure resiliency.

Questions to consider internally:

How do you recognize critical services?

Do you identify and document resilience requirements for the delivery of critical services?

How is resiliency reflected in Service Level Agreements?

Recommendations:

Document a process to identify systems as being "critical" to the organization. Determine controls to put in place to maintain these systems and services. Service Level Agreements (SLAs) should appropriately reflect your ability to provide service. Be able to demonstrate evidence of controls to ensure acceptable downtimes are met.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

IT SECURITY POLICY & STANDARDS – Formal IT Security policies, standards, and procedures exist and are made available to all applicable parties.

IT security policies and standards establish the foundation for an IT security program. This documentation serves as the basis for being able to provide evidence of due care and due diligence, which is critical for any business that is regulated or accepts payment cards (e.g., PCI DSS).

Questions to consider internally:

Does a formal IT security policy exist?

Is the policy supported by formal procedures?

Is the policy periodically communicated to all relevant employees and external business associates?

Recommendations:

IT Security Policy, Standard, or Procedures document should be in place with evidence of annual reviews. Be able to produce evidence of management support and that the Policy made available to all users. Failure to adequately document IT security policies and procedures may result in regulatory non-compliance, lack of accountability, lapses in security coverage, unmitigated vulnerabilities, ad-hoc response processes, and poor visibility into security precautions.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

IT SECURITY ROLES & RESPONSIBILITIES – Coordinate and align internal and external IT Security roles.

Having a single point of contact or an assigned group/team is crucial to avoid assumptions about who is taking care of security concerns. Coordination and alignment is the next step for roles and responsibilities, following identify.

Questions to consider internally:

Are there documents that clearly define job functions and responsibilities?

Do these functions complement one another?

Recommendations:

Develop job descriptions and associated responsibilities for IT security staff or IT staff with information security responsibilities. Include documentation of assignment orders for individuals to fill certain information security roles and requirements to perform the information security roles and responsibilities.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

REGULATORY & NON-REGULATORY REQUIREMENTS – Adhere to all applicable requirements.

Monitor the legislative and industry landscape to ensure security policy is updated in consideration of changes that are pertinent or applicable to the organization. Facilitate any validation audits, assessments or reporting that is necessary to assure compliance to applicable laws, regulations, or requirements. Includes the HIPAA Privacy Office(r), IRS Safeguard Reviews, and responses to third party inquiries into the security of the organization.

Questions to consider internally:

Does the organization adhere to applicable regulatory and non-regulatory requirements?

How do you know if a requirement applies to you or not?

Recommendations:

Maintain documentation or attestation of awareness to applicable information security laws and requirements (e.g., PCI DSS). If applicable, keep evidence of current compliance with applicable laws and requirements.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

IT SECURITY PROGRAM – Develop a program to govern cybersecurity risks.

The farther along a company gets with its level of IT maturity, a formal program should exist to properly manage IT security-related risks.

Questions to consider internally:

Is there an IT security program to govern cybersecurity risk?

Does the organization provide funding and resources as needed to support the Security Program?

Recommendations:

Consider this best practice an over-arching concept. An IT Security Program covers the processes, people, and technology working in concert to establish the level of security required for the business to operate as needed. Maintain documentation of a formal information security program to not only leverage it as a market differentiator for you, but also as evidence of regulatory compliance.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

VULNERABILITY IDENTIFICATION – From installing missing patches to scanning for vulnerabilities, it is critical for businesses to understand technical weaknesses by identifying and correcting vulnerabilities as those are found.

The farther along a company gets with its level of IT maturity, a formal program should exist to properly manage IT security-related risks.

Questions to consider internally:

Can you describe the process implemented for identifying vulnerabilities?

Have resource and asset vulnerabilities been identified?

Recommendations:

Implement a viable and repeatable process for managing software patches and remediating vulnerabilities. Maintain documentation of a vulnerability management program/ process as part of the IT Security Policy within the IT Security Program.

Don't forget to take notes!

THREAT & VULNERABILITY INTELLIGENCE – Receive threat and vulnerability information from quality sources.

As part of the VMP, sign up for any of numerous feeds to receive the latest threat and vulnerability information. These feeds can help highlight a vulnerability so that it can be remediated, prior to a hacker being able to exploit it.

Questions to consider internally:

What are the methods in place to receive threat and vulnerability information as necessary?

How is new information incorporated into the Vulnerability Management Program?

Recommendations:

Subscribe to numerous threat feeds to receive threat and vulnerability information. Implement guidelines to determine how much of a threat this new information is.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

THREAT ASSESSMENTS – Address both internal and external threats as part of the VMP.

Threat assessments evaluate systems and applications in terms of design and architecture to ensure that current and anticipated threats are mitigated within acceptable risk tolerances. This includes an analysis of in-place systems periodically or when significant change occurs as well as the analysis of the introduction of new technology systems.

Questions to consider internally:

Have resource and asset vulnerabilities been assessed?

Are the assessments conducted as part a current Business Impact Analysis (BIA), Risk Assessment (RA), Threat Assessment, or similar process?

Recommendations:

Align risk management with an organization-wide framework. Maintain documentation that threats to organizational assets (both internal and external) are identified and assessed. Regularly assess threats as part of the Vulnerability Management Program.

Don't forget to take notes!

BUSINESS IMPACT ASSESSMENT (BIA) – Assess the likelihood and impact associated with inherent and residual risk as part of the VMP.

Business Impact Assessments (BIA) are instrumental in helping businesses understand risk in their IT environments. BIAs consider all available risk sources (e.g., audit results, threat and vulnerability analysis, and regulatory compliance) and allow companies to think through actions and identify courses of action, in case something negative occurs.

Questions to consider internally:

Has a Business Impact Analysis been conducted?

Is there documentation that identifies critical business functions, impact of the loss of that function, the interdependencies between those critical functions and recovery objectives and timeframes?

Recommendations:

As part of the Vulnerability Management Program (VMP), Business Impact Assessments (BIA) are performed to assess the likelihood and impact associated with inherent and residual risk, considering all available risk sources. Maintain documentation or attestation that BIAs are being performed.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

RISK DETERMINATION – Use threats, vulnerabilities, likelihoods and impacts to determine risk as part of the VMP.

Risk needs to be evaluated/assessed to ensure that business operations are capable of delivering services efficiently and effectively within acceptable tolerances. This helps to define risk in the organization.

Questions to consider internally:

Does a document exist which outlines risks, business processes at risk/exposed, alternatives to reduce risks, and tolerance for risks?

Recommendations:

Maintain documentation of a risk assessment program and its output.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

RISK RESPONSES – Identify and prioritize risk responses as part of the VMP.

A well-thought risk program identifies potential or likely scenarios and the organization identifies appropriate responses, should the scenario actually occur.

Questions to consider internally:

Are responses to risk identified and prioritized?

Is this document available as needed for review?

Recommendations:

Maintain a current Business Impact Analysis (BIA), Risk Assessment (RA), or Threat Assessment as documentation of a risk assessment program.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

RISK MANAGEMENT FRAMEWORK – Implement an enterprise-wide Risk Management Framework (RMF) to manage risk to an acceptable level.

A Risk Management Framework (RMF) is essentially a plan that ties the various risk assessment components together so that risk can be managed to an acceptable level. The RMF is more management-focused, as compared to the Vulnerability Management Program (VMP) which is technically-focused and a sub-component of the RMF.

Questions to consider internally:

Is risk acceptably managed at the enterprise level?

How does the RMF assist in making the determination that risk is acceptably managed?

Recommendations:

Maintain a current Business Impact Analysis (BIA), Risk Assessment (RA), or Threat Assessment as documentation of a risk management framework.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

RISK TOLERANCE LEVEL – Determine and document risk tolerance as part of the RMF.

Management is responsible for determining an acceptable level of risk. Acceptable risk may be governed by applicable regulatory or non-regulatory requirements.

Questions to consider internally:

Has the risk tolerance level of the organization been determined and documented?

Recommendations:

Maintain documentation of a risk assessment program within the IT Security Policy. Within that documentation, define what "acceptable risk" is to the organization and who can make that judgment.

Don't forget to take notes!

IDENTIFY: GOVERNANCE

RISK THRESHOLDS – Identify and document thresholds for incident alerts as part of the RMF.

Through assessing risk-based scenarios, management is able to identify what is acceptable and what is unacceptable risk. These scenarios help identify junctions where escalation to higher management is necessary to address the level of risk involved.

Questions to consider internally:

Have incident alert thresholds been determined and documented?

What is the process used to determine appropriate risk thresholds?

Recommendations:

Don't expect to get this exactly correct the first time through. Present multiple scenarios and research common ways other organizations have been over exposed. Maintain documentation of a risk assessment program within the IT Security Policy, define what "acceptable risk" is to the organization and who can make that judgment.

Don't forget to take notes!

Category 2

Protect

Now that the assets, roles, and processes have been identified, it is time to consider the protections needed to keep those pieces intact.

The PROTECT section details the protection measures needed to demonstrate due diligence in protecting the network and data. Access, design, training, planning, and management support all play a role in effective protection from security events.

Protect has been broken down into 6 sub-categories: **Access Control, Training, Data Protection, Processes & Controls, Management,** and **Maintenance Protections**.

PROTECT: ACCESS CONTROL

LOGICAL ACCESS CONTROL – Manage credentials to ensure access is limited to authorized users/devices.

Logical access control establishes the standards for the creation, monitoring, control, and removal of accounts. This encompasses the request process for accounts that includes authorization, approval for access by data owners, and acknowledgement of the user of their responsibilities. Periodic reviews of access permissions, as well as prompt removal of access during role change or employment termination, are also part of account management.

Questions to consider internally:

Are logical access controls managed to ensure authorized access?

When considering the management, how is the process implemented and reviewed?

Recommendations:

Document the policies, standards and procedures used to manage logical access control within the IT Security Policy. Be able to produce evidence of periodic user permission reviews as needed. Managing access control is vital to prevent an inability to investigate incidents, unauthorized access, data loss, lack of accountability, lapses in security coverage, and improperly managed risk.

Don't forget to take notes!

PROTECT: ACCESS CONTROL

PHYSICAL ACCESS CONTROL – Limit physical access to assets and resources to authorized users.

Physical access control establishes the standards for managing physical access to the organization's facilities by all parties (e.g., employees, customers, guests and vendors).

Questions to consider internally:

Are mechanisms in place to limit physical access to authorized users?

How are the mechanisms documented?

Recommendations:

Document the policies, standards and procedures used to manage physical access control within the overall IT Security Policy. Similar to logical access control, physical access control can play a key role in data loss prevention.

Don't forget to take notes!

PROTECT: ACCESS CONTROL

REMOTE ACCESS CONTROL – Limit remote network access to authorized users and devices.

Remote access control establishes the standards for managing remote access to the organization's networks by all parties (e.g., employees, partners, vendors, etc.).

Questions to consider internally:

Is remote network access limited to authorized users?

How are those policies enforced?

Recommendations:

Document the policies, standards and procedures used to manage remote access within the overall IT Security Policy.

Don't forget to take notes!

PROTECT: ACCESS CONTROL

LEAST PRIVILEGE – Permissions are managed with principles of least privilege and separation of duties.

A fundamental tenet of good IT security is to limit privileges to only those users or services that need access. Access is meant to be limited to authorized users, processes acting on behalf of authorized users, or authorized devices. Role Based Access Control (RBAC) is an example of enforcing least privilege.

Questions to consider internally:

Are the principles of least privilege and separation of duties followed in regards to logical and physical access permissions?

Recommendations:

Document the policies, standards and procedures used to Role Based Access Controls (RBAC) within the overall IT Security Policy.

Don't forget to take notes!

PROTECT: ACCESS CONTROL

NETWORK SEGMENTATION – Implement and segregate the network.

The concept of segmenting or segregating a network is a technical way to enforce the concepts of least privilege and least access, since it prevents unauthorized traffic from traversing the network, which could do harm to the company.

Questions to consider internally:

Is the network segregated and segmented?

What guiding principles are used to assist in segmentation?

Recommendations:

If segmentation is applicable, you will want documentation or attestation that logical and/or physical partitioning is used for segregation/segmentation. Segmentation is tied to the level of acceptable risk and compliance requirements as well as best security practices.

Don't forget to take notes!

PROTECT: TRAINING

AWARENESS & TRAINING – Provide cybersecurity training and awareness for all users.

It is critical to effectively and constantly educate the organization on information security precautions, privacy requirements, and information related to the protecting organizational assets.

Questions to consider internally:

Is there a program in place to train and reinforce awareness for all users?

Recommendations:

CompTIA and others provide non-technical training for cybersecurity awareness. Invest in a program focused on teaching smart internet security techniques for all users. Maintain documentation of policies, standards and procedures used to manage information security training & awareness. You can leverage evidence of periodic user training/awareness in market differentiation.

Don't forget to take notes!

PROTECT: TRAINING

PRIVILEGED USER TRAINING – Adequately prepare privileged users for their specific cybersecurity roles.

How are privileged users trained in their specific cybersecurity roles and responsibilities?

Questions to consider internally:

How are privileged users trained in their specific cybersecurity roles and responsibilities?

Recommendations:

Maintain documentation of training on procedures for users with elevated privileges to ensure they understand the additional responsibilities that come with administrative rights.

Don't forget to take notes!

PROTECT: TRAINING

SERVICE PROVIDER TRAINING – Third-parties understand their specific cybersecurity roles.

Validating service providers are properly trained may Include contract review, as well as the development of service level agreements and requirements. Since service providers are become crucial to business operations, service providers need to understand and abide by their roles and responsibilities.

Questions to consider internally:

Has the potential impact of 3rd parties been evaluated from a risk assessment perspective?

Are third-parties adequately trained and made aware of their roles and responsibilities, if applicable?

Recommendations:

If applicable, be able to address how 3rd party training is handled and maintain documentation that identifies third-party stakeholder roles and responsibilities for information security.

Don't forget to take notes!

PROTECT: TRAINING

MANAGEMENT TRAINING – Prepare management and executives for their specific cybersecurity roles.

Educating an organization's management on IT security topics specific to their management roles and responsibilities is very important. This reduces confusion and assumptions around IT security topics, as well as controls that may or may not be in place to protect the organization.

Questions to consider internally:

What topics have been identified as specific to management?

Is management trained for their specific roles and responsibilities?

Recommendations:

Maintain documentation or attestation that training or procedures for management or executives exist to ensure they understand the additional responsibilities that come with the oversight of the organization's information security program. Include the policy prescribing management training within the overall IT Security Policy.

Don't forget to take notes!

PROTECT: TRAINING

SECURITY PERSONNEL TRAINING – Train and prepare for their specific cybersecurity roles & responsibilities.

To ensure that IT security personnel are kept abreast of the latest threats and countermeasures, as well as understanding the tools they use to perform their duties, it is important to ensure IT security personnel are adequately prepared.

Questions to consider internally:

How is security personnel kept up-to-date with the latest information?

Are security personnel trained for their specific roles and responsibilities?

Recommendations:

Define additional policy requirements for security personnel within the overall IT Security Policy. Maintain documentation or attestation that awareness or other programs exist to ensure personnel with IT security roles are properly trained to fulfill their responsibilities. This may include, but is not limited to: computer based training, webinars, or certifications.

Don't forget to take notes!

PROTECT: DATA PROTECTION

PROTECTING DATA-AT-REST

Protecting data at rest is most commonly implemented in a form encryption (e.g., whole drive or file). While it is an evolving best practice, some industries and jurisdictions require encrypting sensitive data at rest.

Questions to consider internally:

What protections are in place for data-at-rest?

Recommendations:

Put in place, and maintain documentation that sensitive Personal Identifiable Information (PII) is protected with some form of encryption. In case of auditing, this may be a screenshot or it could be an attestation of the type of encryption in use and the scope of its implementation. House these policies within the overall IT Security Policy.

Don't forget to take notes!

PROTECTING DATA-IN-TRANSIT

Protecting data in transit takes on many forms, most commonly is using VPNs to secure remote work connections or HTTPS to secure online purchases. The intent is to implement encryption whenever possible to protect data in transit.

Questions to consider internally:

What protections are in place for data-in-transit?

Recommendations:

Maintain documentation that a type of encryption is used to implement point-to-point encryption or other methods of encrypting data-in-transit. House this in the overall IT Security Policy.

Don't forget to take notes!

PROTECT: DATA PROTECTION

REMOVAL OF ASSETS & DATA – Manage the removal, transfer, and disposal of assets and resources.

Without controlling the removal of assets from an organization's facilities, it makes physical access control nearly impossible. This greatly increases the risk of a data breach due to the loss of assets that contain sensitive information.

Questions to consider internally:

What mechanisms are in place to manage the removal, transfer, and disposal of assets and resources?

Recommendations:

Maintain documentation that describes the approved method(s) to remove, transfer or dispose of assets and resources. An example of a record to maintain would be a contract from a document destructions company. Whatever the implemented policy, include it in the overall IT Security Policy.

Don't forget to take notes!

PROTECT: DATA PROTECTION

AVAILABILITY PROTECTIONS – Ensure adequate availability capacity is maintained.

Many businesses have mechanisms in place to protect the up-time of their Internet presence (e.g., websites, email, services, etc.) and availability protections can take the form of redundant circuits, failover hardware and Distributed Denial of Service (DDoS) prevention.

Questions to consider internally:

What mechanisms exist to ensure availability?

Recommendations:

Maintain documentation to demonstrate that steps are taken to ensure uptime is protected. This may include redundant hardware or telecommunications connections. Proper availability protections will help limit business interruption and improve responses to incidents that may arise.

Don't forget to take notes!

DATA LEAKAGE – Protect against data leakage.

Data leakage can come in the form of a misconfiguration of a firewall or a poorly constructed website. All companies have to be aware of what potentially sensitive information is leaking from their networks and websites for hackers to pick up.

Questions to consider internally:

How is data leakage identified?

What mechanisms are in place to protect against data leakage?

Recommendations:

Communicate to employees what they are allowed and/or prohibited from posting to the internet or sharing over email, etc. Maintain documentation that covers that information within the overall IT Security Policy. Implement a vulnerability management plan that covers how results from external vulnerability scans are reviewed for signs of data leakage.

Don't forget to take notes!

INTEGRITY CHECKING – Verify software, firmware, and information integrity.

Information security integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering).

Questions to consider internally:

What mechanisms are in place to verify information and data integrity?

Is there a commercial product in place to assist?

Recommendations:

Maintain documentation that business-class hardware and software are being used, since commercial products include integrity checking mechanisms. Otherwise, be able to identify the mechanisms in place to conduct integrity checks.

Don't forget to take notes!

PROTECT: DATA PROTECTION

SEPARATE ENVIRONMENTS – Separate development/testing from production environment.

The security of production networks justifies a separate network for development or testing. This allows for mistakes or misconfigurations in the test/dev environments from compromising or taking down the production network.

Questions to consider internally:

How are development/testing environments separated from production?

Recommendations:

Maintain documentation that describes the separation between the production network and any test, development or staging networks such as a network diagram.

Don't forget to take notes!

PROTECT: DATA PROTECTION

BASELINE CONFIGURATION REQUIREMENTS – Utilize standards based on industry best practices.

Baseline configurations establish and enforce security configuration settings for information technology products and ensures all systems are operating under configurations that have been agreed upon according to organizational risk management.

Questions to consider internally:

Have baselines been established?

Were industry best practices used in setting baseline configurations?

Do the baselines operate in line with the risk management strategy?

Recommendations:

Maintain documentation that IT security configuration baselines being tested, approved, uniformly implemented and maintained across the organization.

Don't forget to take notes!

SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) – Implement and manage a System Development Life Cycle.

The integration of information security requirements and associated security controls into the information security architecture helps to ensure that security considerations are addressed early in the system development life cycle and are directly and explicitly related to mission/business processes.

Using a roadmap and emerging technology evaluation process, a System Development Life Cycle (SDLC) allows organizations to stay abreast of the continued evolution of security solutions, processes, and technology to identify continuous, ongoing ways to deliver technology and information securely.

Questions to consider internally:

Do you utilize a System Development Life Cycle (SDLC)?

Recommendations:

Implement a SDLC or computer lifecycle plan to manage assets and applications. Maintain documentation of the SDLC and its policies within the overall IT Security Policy.

Don't forget to take notes!

CONFIGURATION CHANGE CONTROL – Implement and manage a configuration change control process.

Configuration change control establishes a set of rules and administrative guidelines to manage changes in a rational and predictable manner. In addition, it provides for the necessary documentation of any changes made so as to reduce any possible negative impact to the users. Changes include, but are not limited to implementation of new functionality, interruption of service, repair of existing functionality, and the removal of existing functionality.

Questions to consider internally:

What change control processes are in place?

Recommendations:

Establish two branches of change management – one for internal use and one for customers/clients. Maintain documentation that change control processes exist and are used within the overall IT Security Policy.

Don't forget to take notes!

PROTECT: PROCESSES & CONTROLS

DATA BACKUP – Conduct, maintain, and test in accordance with policies and standards.

Backing up data and applications is a business requirement. It enables the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors).

Questions to consider internally:

Are data backups handled according to policy?

Recommendations:

Defining and documenting a policy for the frequency and process for data backup is important to maintain data integrity and prevent data loss. Maintain documentation that a data backup plan exists and is used. In record-keeping, have evidence of routine testing of backups. House the backup policy within the overall IT Security Policy.

Don't forget to take notes!

WORKPLACE SECURITY – Security controls and mechanisms are effective regardless of workplace.

Workplace security encompasses physical access to information systems, equipment, and the respective operating environments. Physical locations and support infrastructure for information systems require protections, since computing is no longer limited to traditional workstations. Mobile computing has introduced tablets, smartphones, handhelds and other computing devices designed to be portable and facilitate productivity for remote users. Traditional controls still apply in many areas, but additional considerations must be made for portable devices and the specific configuration and enforcement of controls will likely require special consideration.

Questions to consider internally:

How have the variety of workplaces been identified?

Have all potential workplaces been considered as related to security controls and mechanisms?

Recommendations:

Maintain documentation that security controls are effective for remote workers or users who take laptops/tablets home. You should look for how security is effective away from the office as well as in the office.

Don't forget to take notes!

SECURE DISPOSAL OF INFORMATION – Destroy data in a manner that prevents unauthorized disclosure.

Different nations have laws and regulations addressing the destruction of data. In the US, Federal laws such as FACTA and HIPAA, and several state laws take the disposal of sensitive information very seriously. Sensitive data that could lead to identity theft must be disposed of in a manner that makes recovery technically impossible.

Questions to consider internally:

Are you aware of local and national disposal requirements that may impact the organization?

Is data destroyed in a secure manner?

Recommendations:

Maintain documentation of data destruction policy/standards/procedures, including a policy housed in the overall IT Security Policy. Make evidence of document/asset destruction available upon request as appropriate. One way to help meet this standard is to contract with a data destruction vendor that specializes in secure disposal.

Don't forget to take notes!

PROTECTION EFFECTIVENESS REVIEW – Appropriate parties are made aware of the effectiveness of protection mechanisms.

Key stakeholders (e.g., customers, partners, vendors, etc.) should be kept aware of the results of ongoing reviews of the IT security program's effectiveness.

Questions to consider internally:

Are protection processes regularly reviewed for improvement?

Recommendations:

Management should periodically review how effective IT security controls really are. This may be a review of incidents over the past year or even attempting to bypass technical controls to see if those can be circumvented. This is all part of an ongoing risk assessment process. Maintain documentation of a review process to see how effective the security program and its controls were. May be a component of the overall risk management program.

Don't forget to take notes!

PROTECT: MANAGEMENT

INCIDENT RESPONSE & BUSINESS CONTINUITY PLANS – Incident Response Plans (IRP) and Business Continuity Plans (BCP) are in place and managed.

Plans for emergency response, backup operations, and post-incident occurrence recovery for information systems need to be established, maintained and effectively implemented to ensure the availability of critical information resources and continuity of operations in emergency situations.

Questions to consider internally:

Do you have an Incident Response Plan (IRP)?

Do you have a Business Continuity Plan (BCP)?

Do you have a Disaster Recovery Plan (DRP)?

Recommendations:

These plans are vital to the ongoing activities of the business and can often be the most imposing challenge for preparation. Spend time researching the nuances of each plan and reach out to your peers for insight and thoughts on how to approach the plans. Maintain documentation of all 3 to assist in response and backup. If necessary, consider an external expert to handle business continuity.

Don't forget to take notes!

PROTECT: MANAGEMENT

RESPONSE & RECOVERY PLAN TESTING – IRP and BCP are tested to ensure validity.

The only way to know for certain if a recovery plan will work is to test it. This should be at least an annual validation that incident response and recovery plans work effectively and efficiently.

Questions to consider internally:

Has the Incident Response plan been tested?

Has the Business Continuity plan been tested?

Recommendations:

Conduct annual or bi-annual testing and mock runs of the plans to make sure they continue to make sense. Maintain documentation that testing occurs to the best of your ability.

Don't forget to take notes!

PROTECT: MANAGEMENT

HUMAN RESOURCES ALIGNMENT – HR processes and procedures incorporate cybersecurity best practices.

Any individual occupying a position of responsibility within the organization (including third-party service providers) needs to be trustworthy and meet established security criteria for that position. HR alignment ensures that information resources are protected during and after personnel actions such as terminations and transfers.

Questions to consider internally:

How do human resources processes incorporate the organization's cybersecurity policies and procedures?

Recommendations:

A great way to encourage proper cybersecurity behavior is to support that goal through HR functions. For example, including formal sanctions for personnel failing to comply with security policies and procedures. You should be able to point to documentation of how HR incorporates cybersecurity best practices into HR processes.

Don't forget to take notes!

PROTECT: MANAGEMENT

VULNERABILITY MANAGEMENT PLAN (VMP) – Develop and implement a Vulnerability Management Plan.

A Vulnerability Management Program (VMP) is a way to keep on top of managing vulnerabilities. VMP is more technically-focused and is a sub-component of the overall Risk Management Framework (RMF).

Questions to consider internally:

Has a Vulnerability Managed Plan been developed?

Recommendations:

Refer back to the best practice in Identify: Governance, where the vulnerabilities were to be identified as part of a larger VMP. This best practice is addressing the VMP itself. Maintain documentation of a Vulnerability Management Plan (VMP) that covers how vulnerabilities are identified, documented and remediated.

Don't forget to take notes!

PROTECT: MAINTENANCE PROTECTIONS

MAINTENANCE SUPPORT – Maintenance of assets and resources is performed.

Ensuring that systems are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and service disruptions is a key component to IT security. This includes configuring operation systems and software with appropriate parameters, removing default accounts/passwords, disabling unnecessary protocols/ports, and the ongoing distribution and installation of service packs.

Questions to consider internally:

How are assets and resources maintained?

Recommendations:

Maintain documentation of ongoing maintenance operations. Include evidence of a patch management and remediation actions following finding vulnerabilities in systems or applications.

Don't forget to take notes!

PROTECT: MAINTENANCE PROTECTIONS

REMOTE MAINTENANCE – Remote maintenance of assets and resources is performed in an approved manner that prevents unauthorized access.

In direct support to maintenance support, remote maintenance takes on unique security concerns due to the remote nature of the support. This focuses on ensuring remote parties only have access to what they need to perform maintenance and that they disconnect when the session is complete.

Questions to consider internally:

Is remote maintenance of assets performed in a secure manner?

Recommendations:

Maintain documentation for how remote maintenance is kept secure, both for internal systems and for client systems. Identify methods of validation to ensure remote maintenance is configured correctly and will prevent unauthorized access.

Don't forget to take notes!

PROTECT: MAINTENANCE PROTECTIONS

AUDIT & LOG RECORDS – Create, protect, and retain logs in accordance with the policies and standards.

Without the ability to review audit logs, putting together the facts of what happened in an incident is nearly impossible. This is why having the proper logging enabled for the correct time duration is a fundamental component to IT security.

Questions to consider internally:

Are logs managed according to policy?

Recommendations:

Maintain documentation of how the organization reviews and retains logs. Include the processes, including roles & responsibilities, for how logs will be reviewed. House these policies in the overall IT Security Policy.

Don't forget to take notes!

REMOVABLE MEDIA – Restrict use of removable media through administrative and technical measures.

Access to digital and non-digital information system media need to be limited to authorized users. This requires that safeguards be in place to restrict access to this media which includes both digital media (e.g., systems, diskettes, magnetic tapes, external/removable hard drives, flash drives and other portable mass storage devices, compact disks) and non-digital media (e.g., paper, microfilm).

Questions to consider internally:

How do administrative and technical measures help restrict removable media usage?

Recommendations:

Maintain documentation of how removable media is secured. Consider options like remote storage, access, cloud services, and VPN to assist securing removable media.

Don't forget to take notes!

LEAST FUNCTIONALITY PROTECTIONS – Secure configurations enforce the principles of least functionality.

Least functionality is a common sense requirement where the functionality of a system, service or application is limited to what is necessary. If everything runs as an administrator/root, a compromise from malware will run with those same privileges, so limiting functionality can drastically reduce the impact of malware and other unauthorized actions.

Questions to consider internally:

How is least functionality enforced in secure configurations?

Recommendations:

Maintain documentation of how least functionality is implemented. References for best practices used to harden systems (e.g., CIS, DISA STIGs, vendor guides, etc.).

Don't forget to take notes!

PROTECT: MAINTENANCE PROTECTIONS

NETWORK COMMUNICATIONS PROTECTIONS – Protect network communications.

This encompasses the control, monitoring, management and protection of communications and transmissions between information systems. It establishes the requirements for protections such as link encryption, secure file transmission protocols, retention of files on source and destination systems, integrity validation, and restrictions for access at all levels (i.e. user/process, system, and network).

Questions to consider internally:

How are network communications protected?

Recommendations:

Maintain documentation of how communications, PKI, encryption, digital signatures, etc. is secured. There are numerous high-quality commercial products to help achieve this standard.

Don't forget to take notes!

Category 3

Detect

You have now IDENTIFIED the key assets, roles, and processes and established PROTECTIONS for to keep them around and properly functioning. It is now time to consider how to detect incoming threats and incidents in order to prevent, mitigate, or at least halt the progress of an incident.

The DETECT section covers the security controls to detect events that have gotten through protections. Functions such as establishing baselines and thresholds, monitoring, and recognizing what is a threat are detailed.

Detect has been broken down into 3 sub-categories: **Determining an Event, Monitoring,** and **Planning**.

NETWORK TRAFFIC BASELINES – Establish expected data flows to identify what constitutes "anomalous" behavior.

Baselines of network traffic can help organizations identify anomalous network behavior, such as spikes in traffic, unusual protocol usage or traffic to certain network segments.

Questions to consider internally:

Have network traffic baselines been established?

Recommendations:

Maintain documentation of baselines used to identify "anomalous" network traffic. By being familiar with what "normal" looks like, you have an indicator for when something different comes across.

Don't forget to take notes!

DETECT: DETERMINING AN EVENT

ANOMALY DETECTION – Analyze detected events to understand the targets and methods used.

Detecting anomalies is rooted in reviewing logs, either manually or through an automated process. IDS/IPS are especially helpful in identifying anomalies. Having network baselines helps rule out false positives in anomaly detection.

Questions to consider internally:

Are detected events analyzed to understand the target and method?

How is that analysis conducted?

Recommendations:

Include the procedure for analysis within an Incident Response Plan as part of the overall IT Security Policy. Maintain documentation of how detected events are analyzed. Consistent analysis can help anticipate targets and any weak points your security coverage may be missing.

Don't forget to take notes!

DETECT: DETERMINING AN EVENT

EVENT CORRELATION – Improve detection and escalation with information from different sources.

Event correlation is rooted in reviewing logs. This may include checking firewall logs, in conjunction with server logs, to identify the actions a hacker took while attacking a network. Aggregating logs into a Security Incident Event Management (SIEM) console can greatly improve the efficiency of event correlation.

Questions to consider internally:

Is data correlation used to improve understanding of an event?

How are log reviews encouraged as part of a regular checking process?

Is there a specific individual or team assigned?

Recommendations:

Maintain documentation of how events are (if applicable) correlated to other event sources to gain a better understanding of the incident. Pair this activity with the analysis procedure and include it as part of the Incident Response Plan within the overall IT Security Policy.

Don't forget to take notes!

EVENT IMPACT ASSESSMENT – Determine appropriate response based on the potential impact.

Once an event is identified, it is important to understand the potential impact. This is rooted in having qualified and proficient IT security personnel who know how to assess events for potential impacts.

Questions to consider internally:

Are events assessed to determine response based on the impact?

Is there a specific individual or team assigned?

Recommendations:

At this stage of the event, response actions are not yet ready to begin. This best practice addresses understanding the impact of the event and aligning the proper responses based on that impact. Information gathered from the event analysis and event correlation will help shape the overall impact assessment. Maintain documentation of the process used to assess events for possible escalation.

Don't forget to take notes!

DETECT: DETERMINING AN EVENT

INCIDENT ALERTING THRESHOLDS – Establish thresholds to manage incident alerting and escalation.

Management should be aware of incidents and IT security personnel should be provided thresholds for when alerts need to be escalated.

Questions to consider internally:

Are thresholds established to manage incident escalation?

Recommendations:

Establishing and reviewing proper alert thresholds will help keep the proper people informed of situations they need to be aware of. Maintain documentation of the method in which thresholds are used to escalate incidents, and how they are determined and reviewed. Use the Incident Response Plan within the overall IT Security Policy to document the process.

Don't forget to take notes!

DETECT: MONITORING

NETWORK MONITORING – Monitor the network to detect potential cybersecurity events.

Network monitoring encompasses the analysis of security events and alerts as detected by the array of security and log collection devices implemented throughout the network. Security monitoring and analysis includes alert configuration and generation, event correlation as well as defining and distributing periodic reports and event statistical analysis.

Questions to consider internally:

How is network traffic monitored for potential events?

Recommendations:

Maintain documentation of how network traffic is monitored within the overall IT Security Policy. You may also find it beneficial to work with a vendor specializing in this function.

Don't forget to take notes!

DETECT: MONITORING

PHYSICAL MONITORING – Monitor physical area to detect potential cybersecurity events.

Physical monitoring encompasses reviewing physical security logs, including visitor access. Inspections of facilities also can identify potential physical breaches.

Questions to consider internally:

Is the physical environment monitored for potential events?

Recommendations:

This is an easily dismissed and overlooked aspect to security, given so much focus on the network and social engineering protections. But simple, regular reviews of physical locations and workplaces can provide information missed by technical monitoring. Maintain documentation of how facilities are monitored for evidence of potential incidents, such as perimeter checks, looking for signs of break in, etc. You may find it useful to bring on a specific physical security vendor to assist, if the locations are large or numerous.

Don't forget to take notes!

DETECT: MONITORING

PERSONNEL MONITORING – Monitor user activity to detect potential cybersecurity events.

Depending on the risk threshold of the organization, management may monitor user activity for signs of potential cybersecurity incidents.

Questions to consider internally:

How is user activity monitored for potential events?

Recommendations:

Maintain documentation of how user activity is monitored to identify possible cybersecurity incidents. This may include Internet content filtering, time of day usage reviews, etc.

Don't forget to take notes!

DETECT: MONITORING

MALICIOUS CODE DETECTION MECHANISMS – Deploy mechanisms to detect and eradicate malicious code.

The prevention, detection and cleanup of malicious software (e.g., virus, worm, Trojan, Spyware and other similar variants) is a basic business necessity. Protection is accomplished at varying layers including at the host, at the network, or at the gateway perimeter. Protection mechanisms must be updated periodically and frequently to address evolving threats and monitored to provide manual intervention where required.

Questions to consider internally:

What mechanisms are in place to detect and eradicate malicious code?

Recommendations:

Consider tools such as network intrusion prevention systems and network and host-based firewalls to assist in this practice. Technical solutions should align with the business goals of the process behind the task. In other words, make sure the product in place is doing what you need it to do. Maintain documentation of the types of antimalware software deployed on servers, workstations and mobile devices. This includes how the software is kept current and prevents users from disabling protection mechanisms.

Don't forget to take notes!

DETECT: MONITORING

MOBILE CODE DETECTION MECHANISMS – Be able to detect and take corrective actions when unacceptable mobile code is detected.

Depending on the risk threshold of the organization, mobile code may want to be blocked or otherwise acted upon (e.g., blocking, quarantine, or alerting administrators). This entirely depends on how secure an organization wants to lock down its assets and network.

Questions to consider internally:

Is mobile code detectable and managed according to policy?

Recommendations:

Given the rise of mobile devices as integral pieces of the workplace, this best practice calls out specific attention to the need to monitor these devices for different attacks. If applicable, maintain documentation how mobile code is managed.

Don't forget to take notes!

DETECT: MONITORING

SERVICE PROVIDER MONITORING – Monitor providers to ensure conformance with the organization's policies, standards, procedures, and contractual obligations.

This encompasses the due diligence applied to monitoring the performance of service providers and their level of compliance with SLAs or other agreements to the services provided.

Questions to consider internally:

Are third-party providers regularly monitored for adherence to contractual and procedural obligations?

Recommendations:

Have clear documentation and instruction available for 3rd party services to make them aware of their responsibilities and obligations regarding monitoring. Maintain documentation of how service providers are managed to ensure service providers are operating in accordance with policies, standards and procedures.

Don't forget to take notes!

DETECT: MONITORING

PERIODIC CHECKS – Perform checks for unauthorized personnel, network connections, devices and software.

This encompasses spot checking on various aspects of the IT security program. Checking random controls for compliance is a way to determine if actual practices are following written requirements.

Questions to consider internally:

Is there a system to conduct periodic checks to detect unauthorized activity?

Recommendations:

Maintain documentation of how spot checks are performed to validate IT security controls are operating. If controls were found to be broken, what steps were followed to remediate those deficient controls?

Don't forget to take notes!

DETECT: MONITORING

PRODUCTION VULNERABILITY SCANNING – Vulnerability assessment scans are performed.

Vulnerability scanning can broadly include evaluating systems vulnerabilities, patch management levels and basic configuration management. Vulnerability scans (internal and external) is a requirement in the PCI DSS, so it applies to all organizations that accept payment cards.

Questions to consider internally:

Are vulnerability scans performed?

Recommendations:

Products such as web application firewalls, network intrusion prevention systems, and end-point protections can help implement this as a best practice. Maintain evidence of vulnerability scanning being performed on an ongoing basis to help with any compliance audits and for reviewing records.

Don't forget to take notes!

DETECT: PLANNING

ROLES & RESPONSIBILITIES FOR EVENT DETECTION & RESPONSE – Assign personnel responsible for event detection.

Specific to event detection and response, this focuses on having the proper personnel identified and trained in their assigned roles and responsibilities.

Questions to consider internally:

Have personnel responsible for event detection been identified and provided specific roles and responsibilities?

Recommendations:

Maintain documentation on roles and responsibilities for personnel identified for event detection and response. This includes, but is not limited to some form of assignment orders or job description that includes the responsibilities for event detection and response. In an external resource is used for this task, document the vetting and selection process.

Don't forget to take notes!

DETECT: PLANNING

DETECTION PROCEDURES – Appropriate response actions are in line with an Incident Response Plan (IRP).

This encompasses the processes in place that an organization has to detect and respond to incidents.

Questions to consider internally:

Are responses to detection handled according to the Incident Response Plan?

Recommendations:

Within the Incident Response Plan (IRP), the procedures for response to an incident should be defined and available to the people that would need to perform them. These procedures will help limit ad-hoc responses to an incident and demonstrate the due diligence taken ahead of time.

Don't forget to take notes!

DETECT: PLANNING

RESPONSE EXERCISES – Detection processes are tested to ensure that the process is valid.

It is recommended practice to conduct exercises at least annually to ensure personnel understand their roles and responsibilities. This also validates if response plans are realistic.

Questions to consider internally:

Are detection processes tested?

How can testing exercises best replicate real-world situations?

Recommendations:

Testing the efficacy of the Incident Response Plan (IRP) with likely scenarios so that applicable personnel understand their assigned roles and responsibilities for incident response is the best method of evaluating the IRP. Conduct a full de-briefing afterwards to help identify areas of improvement for both the testing and the Plan itself.

Don't forget to take notes!

DETECT: PLANNING

CYBERSECURITY EVENT COORDINATION – Communicate event detection information among appropriate parties.

Generally considered a Cyber Incident Response Team (CIRT), when an incident does evolve and require dedicated resources it is necessary to coordinate response activities.

Questions to consider internally:

Has a Cyber Incident Response Team been identified?

Who is on that team, and why were they chosen?

Recommendations:

If applicable, documentation how a Cyber Incident Response Team (or similar function that responds to incidents) is formed, communicates, and coordinates actions with outside teams/parties. Think of this team as the "go-to" for security incidents. You'll want your best on such a team.

Don't forget to take notes!

DETECT: PLANNING

DETECTION PROCESS IMPROVEMENT – Detection processes are continuously improved.

As part of any program improvement, management should always look for ways to identify areas to improve or gain efficiencies. After Action Review (AARs) from incidents are a great way to document process improvement recommendations. This may include performing a Root Cause Analysis (RCA).

Questions to consider internally:

Are detection processes regularly reviewed?

Recommendations:

Maintain documentation of how After Action Reviews (or similar function that looks to improve actions) are conducted and used to improve incident response processes.

Don't forget to take notes!

Category 4

Respond

The last two categories deal with the aftermath of an incident. Despite all the PROTECTION and DETECTION, you still are at risk of a security incident. How you RESPOND can mean the difference between a minor interruption and catastrophic failure.

The RESPOND section addresses the readiness and ability to respond to a detected event. Analyzing, limiting the impact, and execution of the Incident Response Plan are detailed.

Respond is broken into 3 sub-categories: A**nalysis, Communications,** and **Improvements**.

RESPOND: ANALYSIS

ALERT ANALYSIS – Notifications from detection systems are investigated in a timely manner.

Alert analysis is the action a person takes in an operational incident handling capability that is focused on containment, recovery, and response activities.

Questions to consider internally:

Are notifications investigated?

Recommendations:

Maintain documentation of how alerts from anti-malware, IPS, firewalls, etc. are received and responded to in a timely manner. Include the procedures for this analysis as part of the Incident Response Plan (IRP) within the overall IT Security Policy. You may find it beneficial to retain external assistance in analysis if it is outside the expertise of your organization.

Don't forget to take notes!

RESPOND: ANALYSIS

IMPACT UNDERSTANDING – Evaluate the potential damage and scope of an incident.

Before closing an incident, it is crucial to understand the impact and ensure that proper escalation steps were taken, in accordance with the organization's Incident Response Plan (IRP).

Questions to consider internally:

Are assessments conducted to evaluate the impact of the incident?

Recommendations:

Within the Incident Response Plan (IRP), maintain documentation of how the impact of a potential incident is evaluated as part of the escalation process.

Don't forget to take notes!

RESPOND: ANALYSIS

FORENSICS – Incidents that have the potential for legal action or data breach reporting utilize documented & proper forensic procedures.

Certain types of incidents may necessitate having forensics performed and this requires proper forensic procedures being utilized.

Questions to consider internally:

Is there documentation for handling cases that may require legal action or breach reporting?

If not, how would the implications of such a case impact the organization?

Recommendations:

One of the worst nightmares for a business is to have legal action threaten its existence. While hopefully rare, or even never, proper forensic handling of a breach situation is extremely important for the sake of the business and all its employees. Create and maintain documentation that addresses how sensitive incident response is handled, when the potential for legal action or data breach reporting is suspected.

Don't forget to take notes!

RESPOND: ANALYSIS

INCIDENT CLASSIFICATION – Classify and document incidents consistent with established response plans.

As part of most Incident Response Plans (IRPs), various classifications of incidents are identified and assigned different levels of urgency. This is to ensure serious incidents are handled more urgently than non-serious incidents.

Questions to consider internally:

Is there a classification system in place?

Are incidents classified as required by the response plan?

Recommendations:

Maintain documentation of incident classification types within the IRP so that incidents are properly handled, based on their sensitivity and urgency. Incident classification types can be as simple as malware, lost/stolen asset, misconfiguration, system compromised, etc.

Don't forget to take notes!

RESPOND: COMMUNICATIONS

RESPONSE ROLES & RESPONSIBILITIES – Incident Responders are trained and ready to react when an incident occurs.

Specific to incident response operations, this focuses on having the proper personnel identified and trained in their assigned roles and responsibilities.

Questions to consider internally:

Have personnel assigned for incident response been trained?

Recommendations:

Maintain documentation of the training and readiness of incident response personnel. Consider cross-training response teams to smooth any transition. Remember to emphasize the quality of training of your various teams as market differentiators. Not only can these best practices help achieve a more secure data environment, they can increase business by demonstrating an expertise.

Don't forget to take notes!

RESPOND: COMMUNICATIONS

INCIDENT REPORTING – Events are reported consistent with established criteria in line with the IRP.

Depending on the type of incident and possible legal requirements, a business may have to report an incident to a regulatory body.

Questions to consider internally:

Are events reported according to documented policy?

Recommendations:

Maintain documentation within the Incident Response Plan to demonstrate breach notification is addressed.

Don't forget to take notes!

RESPOND: COMMUNICATIONS

INCIDENT INFORMATION SHARING – Information is shared with appropriate parties.

Depending on the type of incident and possible legal requirements, a business may need to share the specifics of the incident with key stakeholders (e.g., customers, partners or vendors).

Questions to consider internally:

Is information shared according to documented policy?

Recommendations:

Sometimes you will have to communicate not only internally, but externally in response to a security incident. Maintain documentation of a plan to share information with partners, customers, and employees.

Don't forget to take notes!

RESPOND: COMMUNICATIONS

STAKEHOLDER COORDINATION –Response coordination is consistent with documented plans.

Depending on the type of incident and possible legal requirements, a business may need to coordinate with key stakeholders (e.g., customers, partners or vendors).

Questions to consider internally:

Are documented plans used to appropriately coordinate with stakeholders?

Recommendations:

This is the next step after communicating – coordinating a response so all stakeholders are expressing the same things and any potential loose ends or differences can be worked out prior to statements being made. Maintain documentation of a plan to share information with service providers, customers, and other key stake holders.

Don't forget to take notes!

RESPOND: COMMUNICATIONS

SITUATIONAL AWARENESS – Voluntary information sharing with external stakeholders.

Organizations sometimes share information about their incidents with external stakeholders and the industry in general in an effort to raise situational awareness.

Questions to consider internally:

Do you voluntarily share information externally to spread awareness?

Recommendations:

This is a "pay it forward" kind of thing, designed to help the larger community in the case of something new or different in the world of security incidents. If applicable, have a way to easily share useful information with external stakeholders on a voluntary basis. For the receiving end of these types of notices, look for news feeds and threat intelligence sources to help stay abreast.

Don't forget to take notes!

RESPOND: IMPROVEMENTS

INCIDENT RESPONSE LESSONS LEARNED – Incident Response Plan is updated based on lessons learned.

As part of any program improvement, management should always look for ways to identify areas to improve or gain efficiencies. After Action Review (AARs) from incidents are a great way to document process improvement recommendations.

Questions to consider internally:

Are past incidents used to make improvements to the Incident Response Plan (IRP)?

Recommendations:

Updating plans with lessons learned will help make unforeseen adjustments to the plan, which in turn can make it more useful and better. Maintain documentation to demonstrate the Incident Response Plan (IRP) is maintained as lessons are learned and the threat landscape changes.

Don't forget to take notes!

RESPOND: IMPROVEMENTS

INCIDENT RESPONSE STRATEGY UPDATE –Update the Incident Response Strategy.

As people, processes and technologies improve and evolve, it is necessary to periodically update incident response strategies to ensure those plans are appropriate for the organization.

Questions to consider internally:

Do updates to the Incident Response Plan (IRP) include input from multiple sources?

Recommendations:

Maintain documentation to demonstrate the Incident Response Plan (IRP) is maintained as lessons are learned and the threat landscape changes.

Don't forget to take notes!

RESPOND: IMPROVEMENTS

CONTAIN INCIDENTS – Mechanisms are in place to contain the scope of IT security incidents.

The focus here is to ensure that mechanisms are in place to contain incidents. This may be as simple as having response plans that require infected systems to be unplugged from the network to contain incidents.

Questions to consider internally:

Are mechanisms in place to contain the scope of an incident?

Recommendations:

Maintain documentation to demonstrate that controls exist to contain incidents.

Don't forget to take notes!

RESPOND: IMPROVEMENTS

MITIGATE INCIDENTS – Mechanisms are in place to mitigate the ramifications of IT security incidents.

If a critical system was unplugged to contain an incident, a mitigation plan should include how the loss of that system can be alleviated. Be sure to consider other mitigations and their impact.

Questions to consider internally:

Are mechanisms in place to mitigate the impact an incident?

Recommendations:

Maintain documentation to demonstrate that controls exist to mitigate the effect of incidents.

Don't forget to take notes!

RESPOND: IMPROVEMENTS

NEW VULNERABILITY RESPONSE – New vulnerabilities are identified, documented, and mitigated.

The focus here is responding to new vulnerabilities. This can be as simple as ensuring patches are installed once new patches are released and is all part of the Vulnerability Management Program (VMP).

Questions to consider internally:

Are new vulnerabilities managed in a timely manner?

Recommendations:

Maintain documentation to demonstrate that as new vulnerabilities are identified, those vulnerabilities are documented and mitigated in a timely manner. This should be part of the Vulnerability Management Program within the overall IT Security Policy.

Don't forget to take notes!

RESPOND: IMPROVEMENTS

RESPONSE PLAN EXECUTION – For incidents that require response, use a documented IRP.

The focus here is to document Incident Response Plans (IRPs) to be used as reference during incidents, rather than have incidents follow ad-hoc response decisions.

Questions to consider internally:

Are documented plans used to guide incident response?

Recommendations:

A common problem across all industries is failing to execute a plan that has been developed. For security incidents, nothing could be worse. Adherence to the policies, processes, and procedures documented within the plans of the IT Security Policy is the only way to truly live the best practices identified in this standard.

Don't forget to take notes!

Category 5

Recovery

The final phase is RECOVERY. This section has a "wrap-up" feel to it, as you should be shifting your focus from the management of the incident to getting back to full operation and implementing any lessons learned from the experience.

The RECOVERY section details the steps to recover from an event and overcoming any negative fall-out that results. Planning, public and reputation concerns, and getting back to normal are covered.

Recovery has been broken down into 3 sub-categories: **Planning, Improvements,** and **Communication**.

RECOVERY: PLANNING

RECOVERY PLAN – For incidents that require recovery, documented recovery plans are used.

Recovery planning is a methodical process and should be defined and prepared for well before an incident happens

Questions to consider internally:

Are documented plans used to guide recovery from an incident?

Recommendations:

Whether this is addressed in the Incident Response Plan, the Business Continuity Plan, or a Disaster Recovery Plan, the specific steps for recovery from an incident need to be thought through ahead of time and implemented in recovery. Maintain documentation to demonstrate that recovery plans exist and that those plans are viable. If recovery operations happened in the previous year, was the documented recovery plan used?

Don't forget to take notes!

RECOVERY: IMPROVEMENTS

RECOVERY LESSONS LEARNED – Lessons learned from recovery operations are documented and incorporated into future recovery plans.

As part of any program improvement, management should always look for ways to identify areas to improve or gain efficiencies. After Action Review (AARs) from incidents are a great way to document process improvement recommendations.

Questions to consider internally:

Are performed recovery operations used to improve recovery plans?

Recommendations:

This reflects basic process improvement best practices. Maintain documentation to demonstrate that lessons learned from recovery operations were captured and used to improve the overall recovery plan.

Don't forget to take notes!

RECOVERY: IMPROVEMENTS

RECOVERY STRATEGY UPDATE – Lessons learned from recovery operations are used to update response strategies.

As people, processes and technologies improve and evolve, it is necessary to periodically update recovery strategies to ensure those plans are appropriate for the organization.

Questions to consider internally:

Are performed recovery operations used to update response strategies?

Recommendations:

This reflects basic process improvement best practices. Maintain documentation to demonstrate that lessons learned from recovery operations were captured and used to improve the overall strategy.

Don't forget to take notes!

RECOVERY: COMMUNICATIONS

PUBLIC AFFAIRS – Mechanisms are in place to manage public affairs.

Recovery planning should include roles and responsibilities for the possibility of addressing press releases or media inquiries. Improper public affairs responses can be disastrous for organizations.

Questions to consider internally:

Are mechanisms in place to managed public affairs?

Recommendations:

Maintain documentation to demonstrate that the organization is prepared to manage public affairs in the case of an incident that requires public disclosures. This could be specifically assigned personnel to handle PR and the person responsible should have access to the incident reporting and reviews.

Don't forget to take notes!

RECOVERY: COMMUNICATIONS

REPUTATION RECOVERY – Mechanisms are in place to perform reputation recovery.

Similar to public affairs operations, recovery planning should include contingencies for business reputation recovery. This is a business necessity to reassure customers after a publicly visible IT security incident.

Questions to consider internally:

Are mechanisms in place to perform reputation recovery?

Recommendations:

Within the Incident Response Plan, maintain documentation to demonstrate that the organization is prepared to manage public affairs in the case of an incident that requires public disclosures.

Don't forget to take notes!

RECOVERY: COMMUNICATIONS

RECOVERY ACTIVITIES – Recovery activities are communicated to applicable stakeholders.

The focus here is that recovery activities are executed and communicated with the appropriate stakeholders, including executive, management, and cross-functional teams that may act as part of the CIRT.

Questions to consider internally:

Is there a communication plan in place for recovery activities?

Recommendations:

Maintain documentation to demonstrate that the organization has a viable plan in place to communicate recovery activities to applicable stakeholders. Applicable stakeholders includes, but is not limited to customers, vendors, employees, etc.

Don't forget to take notes!

CompTIA

CompTIA Industry Standard: Cybersecurity

WORKBOOK