YOUR LOGO GOES HERE

CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

[NIST SP 800 53 REV5 – LOW, MODERATE & HIGH BASELINES]

ACME Consulting Services, LLP

NIST
SP 800-53 rev5
CSOP
Cybersecurity Standardized Operating Procedures

TABLE OF CONTENTS

KEY TERMINOLOGY

With the Cybersecurity Standardized Operating Procedures (CSOP), it is important to understand a few key terms:

- Procedure / Control Activity: Procedures represent an established way of doing something, such as a series of actions conducted in a specified order or manner. Some organizations refer to procedures as "control activities" and the terms essentially synonymous. In the CSOP, the terms procedure or control activity can be used interchangeably.
- Process Owner: This is the name of the individual or team accountable for the procedure being performed. This identifies the *accountable party to ensure the procedure is performed*. This role is more oversight and managerial.
    - Example: The **Security Operations Center (SOC) Supervisor** is accountable for his/her team to collect log files, perform analysis and escalate potential incidents for further investigation.
- Process Operator: This is the name of the individual or team responsible to perform the procedure's tasks. This identifies the *responsible party for actually performing the task*. This role is a "doer" and performs tasks.
    - Example: The **SOC analyst** is responsible for performing daily log reviews, evaluating anomalous activities and responding to potential incidents in accordance with the organization's Incident Response Plan (IRP).

OVERVIEW

The Cybersecurity Standardized Operating Procedures (CSOP) is a catalog of procedure/control activity statements. These are templates that require slight modification to suit the specific needs of the organization,

CUSTOMIZATION GUIDANCE

The content of the CSOP does require a certain level of customization by any organization, since every organization has some difference in available people, processes or technology that can be leveraged to perform these procedures/control activities.

Essentially, we've done the heavy lifting in developing the template and pre-populating a significant amount of content. Our target is about 80% of the content as part of the template that would leave the remaining 20% for customization with specifics that only the organization would know, such as the organization calls the change management group the Change Advisory Board (CAB) instead of the Change Control Board (CCB). Those little changes in roles, titles, department naming, technologies in use are all content that just needs to be filled into the template to finalize the procedures/control activities.

VALIDATING NEEDS FOR PROCEDURES / CONTROL ACTIVITIES

Procedures are not meant to be documented for the sake of generating paperwork - procedures are meant to satisfy a specific operational need that are complied with:

- If procedures exist and are not tied to a standard, then management should review why the procedure is in place.
- A procedure that lacks a mapping to a standard may indicate "mission creep" and represent an opportunity to reassign the work or cease performing the procedure.

UNDERSTANDING CONTROL OBJECTIVES & CONTROLS

As part of the CSOP, you will see Control Objectives and Controls for each of the CSOP procedures:

- The origin of the Control Objective is ComplianceForge's Cybersecurity & Data Protection Program (CDPP) that consolidates multiple statutory, regulatory and contractual requirements into a single control objective.
- The origin of the Controls is the Secure Controls Framework (SCF) that is an open source set of cybersecurity and privacy controls.

Note - The footnotes at the bottom of the page and the accompanying Excel spreadsheet provide mapping between the control objectives, controls and leading frameworks, including statutory, regulatory and contractual obligations.

PROCEDURES DOCUMENTATION

The objective of the CSOP is to provide management direction and support for cybersecurity in accordance with business requirements, as well as relevant laws, regulations and contractual obligations.

Procedures should be both clearly written and concise.

- Procedure documentation is meant to provide evidence of due diligence that standards are complied with.
- Well-managed procedures are critical to a security program, since procedures represents the specific activities that are performed to protect systems and data.

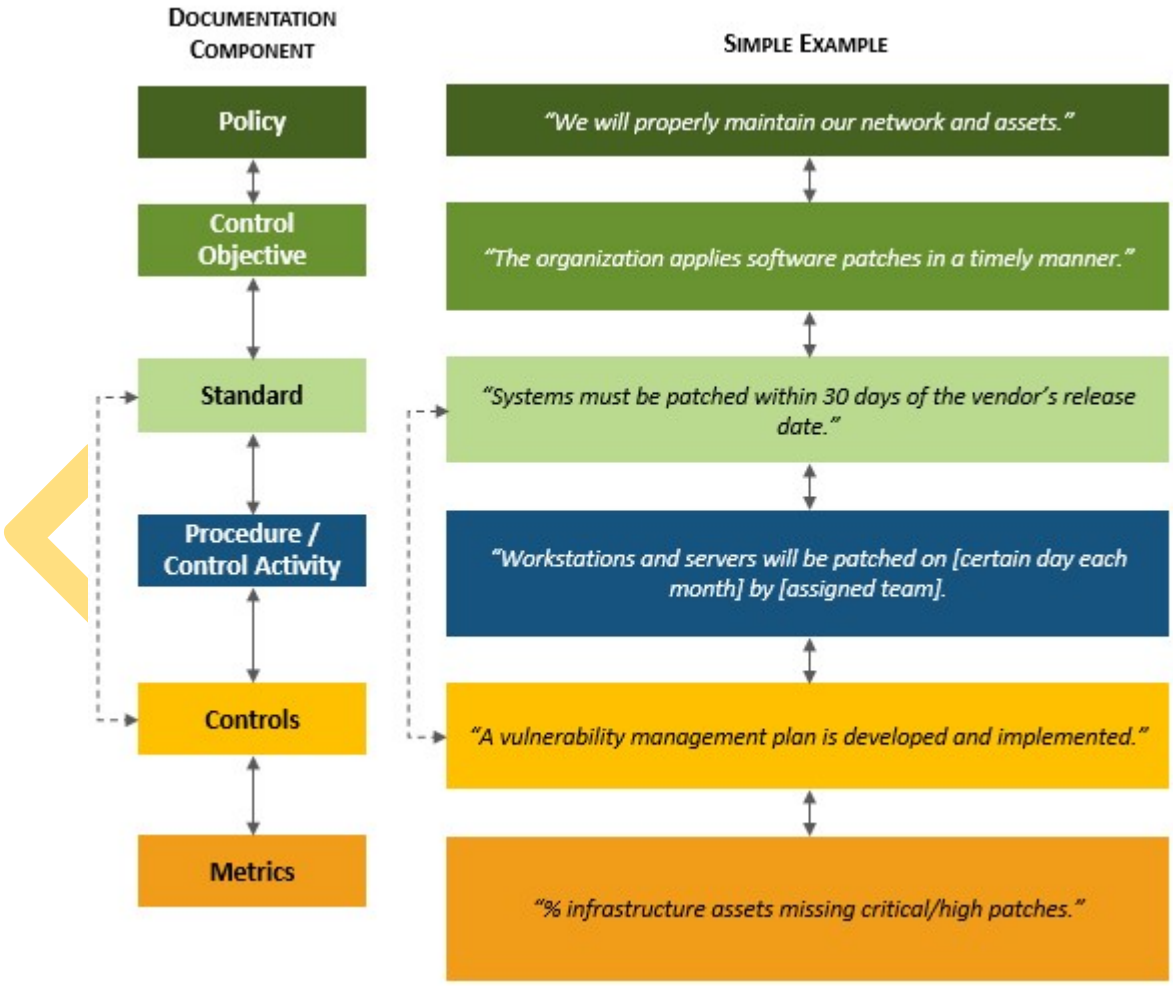
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

From a due care and due diligence perspective, it can be thought of this way:

- Certain standards require processes to exist *(due care – evidence demonstrates standards exist).*
- Performing the activities outlined in a procedure and documenting the work that was performed satisfies the intent of the standard *(due diligence – evidence demonstrates the standard is operating effectively).*

The diagram shown below helps visualize the linkages in documentation that involve written procedures:

- CONTROL OBJECTIVES exist to support POLICIES;
- STANDARDS are written to support CONTROL OBJECTIVES;
- PROCEDURES are written to implement the requirements that STANDARDS establish;
- CONTROLS exist as a mechanism to assess/audit both the existence of PROCEDURES / STANDARDS and how well their capabilities are implemented and/or functioning; and
- METRICS exist as a way to measure the performance of CONTROLS.



Documentation Flow Example.

NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

The CSOP leverages the NIST NICE Cybersecurity Workforce Framework.[1] The purpose of this framework is that work roles have an impact on an organization's ability to protect its data, systems and operations. By assigning work roles, it helps direct the work of employees and contractors to minimize assumptions about who is responsible for certain cybersecurity and privacy tasks.

The CSOP uses the work roles identified in the NIST NICE Cybersecurity Workforce Framework to help make assigning the tasks associated with procedures/control activities more efficient and manageable. Keep in mind these are merely recommendations and are fully editable for every organization – this is just a helpful point in the right direction!

NIST NICE Cybersecurity Workforce Framework – Work Categories

Example Procedure

This example is a configuration procedure **P-CM-2 (Baseline Configurations).**

PLEASE NOTE THE PROCESS CRITERIA SECTION SHOWN BELOW CAN BE DELETED & IS NOT PART OF THE PROCEDURE

The process criteria sections exist only to be a useful tool to help build out the procedures by establishing criteria and creating a working space to capture key components that impacts the procedure.

Process Criteria:

- Process Owner: name of the individual or team accountable for the procedure being performed
  - *Example: The process owner for system hardening at ACME is the cybersecurity director, John Doe.*
- Process Operator: name of the individual or team responsible to perform the procedure's tasks.
  - *Example: The process operator for system hardening at ACME is split between several teams:*
    - *Network gear is assigned to network admins.*
    - *Servers are assigned to server admins.*
    - *Laptops, desktops and mobile devices are assign to the End User Computing (EUC) team.*
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
  - Example: Generally, system hardening is an "as needed" process that happens when new operating systems are released or when new technology is purchased. However, there should still be an annual review to ensure that appropriate baseline configurations exist and are current to what is deployed at ACME.
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
  - Example: The scope affects the entire company. Any deviations to the secure baselines are handled on an individual basis.
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
  - Example: Baseline configurations, benchmarks and STIGs are located on server XYZ123 in the folder called "Secure Baselines" and it is available for read-only for all users.
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
  - Example: There are no SLAs associated with baseline configurations.
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?
  - Example: The following classes of systems and applications are in scope for this procedure:
    - Server-Class Systems
    - Workstation-Class Systems
    - Network Devices
    - Databases

[1] *NIST NICE Cybersecurity Workforce Framework - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework*

Control Objective:[2]

a. Develop, document and maintain under configuration control, a current baseline configuration of the system; and
b. Review and update the baseline configuration of the system:
    1. Per organization-defined frequency;
    2. When required due to organization-defined circumstances; and
    3. When system components are installed or upgraded.

Procedure / Control Activity: Systems Security Developer [SP-SYS-001], in conjunction with the Technical Support Specialist [OM-STS-001] and Security Architect [SP-ARC-002]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure baseline system hardening configuration for all ACME-owned or managed assets comply with applicable legal, statutory and regulatory compliance obligations throughout the System Development Life Cycle (SDLC). [3]

(2) Includes hardware, software, firmware and documentation in baseline configurations. Where technically feasible, technology platforms align with industry-recommended hardening recommendations, including but not limited to: [4]
    a. Center for Internet Security (CIS) benchmarks;
    b. Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs); or
    c. Original Equipment Manufacturer (OEM) security configuration guides.

(3) Ensures that system hardening includes, but is not limited to:
    a. Technology platforms that include, but are not limited to:
        i. Server-Class Systems
            1. Microsoft Server 2003
            2. Microsoft Server 2008
            3. Microsoft Server 2012
            4. Microsoft Server 2016
            5. Red Hat Enterprise Linux (RHEL)
            6. Unix
            7. Solaris
        ii. Workstation-Class Systems
            1. Microsoft XP
            2. Microsoft 7
            3. Microsoft 8
            4. Microsoft 10
            5. Apple
            6. Fedora (Linux)
            7. Ubuntu (Linux)
            8. SuSe (Linux)
        iii. Network Devices
            1. Firewalls
            2. Routers
            3. Load balancers
            4. Virtual Private Network (VPN) concentrators
            5. Wireless Access Points (WAPs)
            6. Wireless controllers
            7. Printers
            8. Multi-Function Devices (MFDs)
        iv. Mobile Devices
            1. Tablets
            2. Mobile phones
            3. Other portable electronic devices
        v. Databases
            1. MySQL
            2. Windows SQL Server
            3. Windows SQL Express
            4. Oracle
            5. DB2

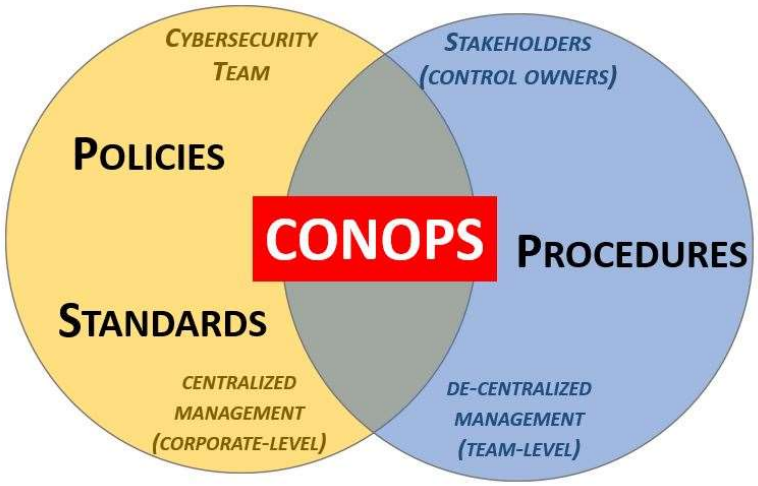
[2] *NIST SP 800-53 Rev 5 control CM-2*
[3] *NIST SP 800-171A assessment criteria 3.4.1[a] & 3.4.1[c]*
[4] *NIST SP 800-171A assessment criteria 3.4.1[b]*

b. Enforcing least functionality, which includes but is not limited to:
    i. Allowing only necessary and secure services, protocols and daemons;
    ii. Removing all unnecessary functionality, which includes but is not limited to:
        1. Scripts;
        2. Drivers;
        3. Features;
        4. Subsystems;
        5. File systems; and
        6. Unnecessary web servers.
c. Configuring and documenting only the necessary ports, protocols and services to meet business needs;
d. Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S-FTP), Transport Layer Security (TLS) or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet and FTP;
e. Installing and configuring appropriate technical controls, such as:
    i. Antimalware;
    ii. Software firewall;
    iii. Event logging; and
    iv. File Integrity Monitoring (FIM), as required; and
f. As applicable, implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers and DNS should be implemented on separate servers).

(4) Documents and validates security parameters are configured to prevent misuse.
(5) Authorizes deviations from standard baseline configurations in accordance with ACME's change management processes, prior to deployment, provisioning or use.
(6) Validates and refreshes configurations on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors. Unless a technical or business reason exists, standardized images are used to represent hardened versions of the underlying operating system and the applications installed on the system.
(7) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(8) If necessary, requests corrective action to address identified deficiencies.
(9) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(10) If necessary, documents the results of corrective action and notes findings.
(11) If necessary, requests additional corrective action to address unremediated deficiencies.

Supporting Policies & Standards

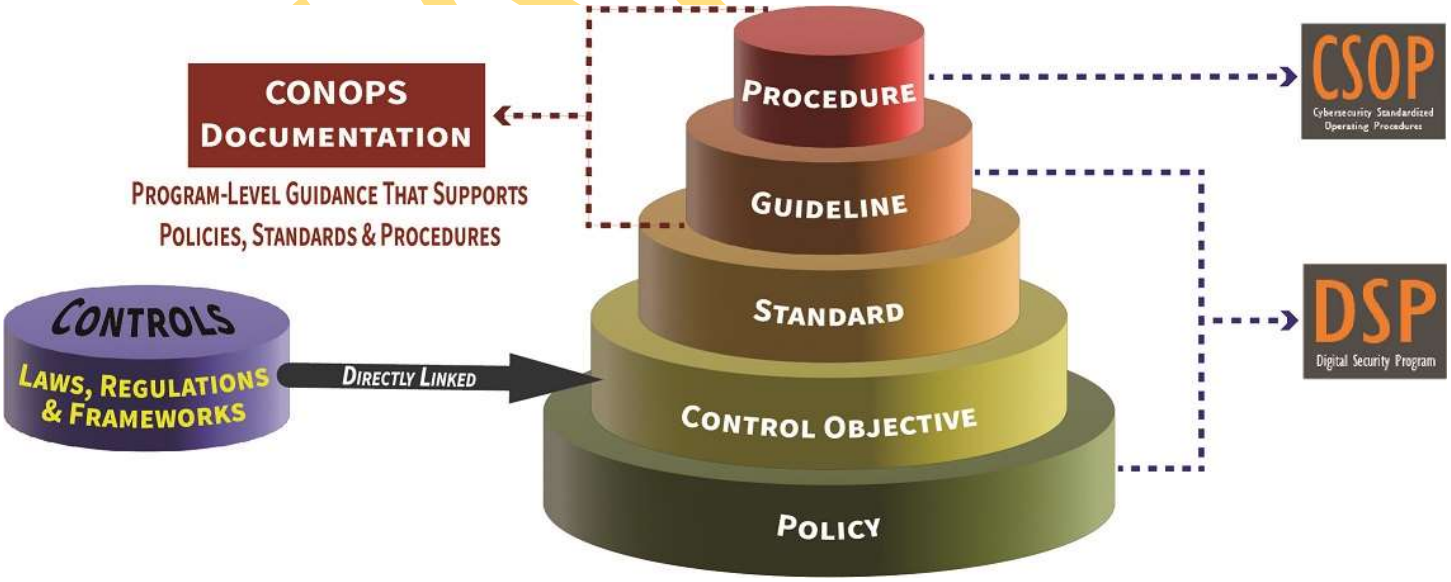
While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with ComplianceForge's NIST SP 800-53-based Cybersecurity & Data Protection Program (CDPP) that contains policies, control objectives, standards and guidelines.



Concept of Operations (CONOPS) relationship.

Cybersecurity documentation is comprised of six (6) main parts:

(1) Core policy that establishes management's intent;
(2) Control objective that identifies leading practices;
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.



Cybersecurity Documentation Hierarchy

As referenced in this graphic, a Concept of Operations (CONOPS) is a security-focused description that addresses life cycle concepts. This can include concepts for sustainment, logistics, maintenance and training. CONOPS augment and support an organization's policies, standards and procedures. Examples of CONOPS documentation includes, but is not limited to:

- Risk management (e.g., Risk Management Program (RMP))
- Vulnerability management (e.g., Vulnerability & Patch Management Program (VPMP))

- Incident response (e.g., Integrated Incident Response Program (IIRP))
- Business Continuity / Disaster Recovery (e.g., Continuity of Operations Plan (COOP))
- Secure engineering practices (e.g., Security & Privacy By Design (SPBD))
- Pre-production testing (e.g., Information Assurance Program (IAP))
- Supply Chain Risk Management (SCRM) (e.g., Third-Party Security Management (TPSM))
- Configuration management (e.g., Secure Baseline Configurations (SBC))

KNOWN COMPLIANCE REQUIREMENTS

ACME has certain compliance requirements that all team members need to be aware of:

STATUTORY REQUIREMENTS

[fill-in applicable statutory requirements]

Example statutory requirements include:

- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Fair & Accurate Credit Transactions Act (FACTA)*
- *Sarbanes Ox ley Act (SOX)*
- *Gramm Leach Bliley Act (GLBA)*
- *Children's Online Privacy Protection Act (COPPA)*
- *Family Educational Rights and Privacy Act (FERPA)*
- *Massachusetts 201 CMR 17.00*
- *Oregon Identity Theft Protection Act (ORS 646A)*
- *United Kingdom Data Protection Act (UK DPA)*

REGULATORY REQUIREMENTS

[fill-in applicable regulatory requirements]

Example regulatory requirements include:

- *Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012)*
- *NIST SP 800-171 / Cybersecurity Maturity Model Certification (CMMC)*
- *Federal Acquisition Regulation (FAR 52.204-21)*
- *European Union General Data Protection Regulation (EU GDPR)*
- *Financial Industry Regulatory Authority (FINRA)*
- *National Industrial Security Program Operating Manual (NISPOM)*
- *Department of Defense Information Assurance Risk Management Framework (DIARMF) (DoDI 8510.01)*
- *Federal Risk and Authorization Management Program (FedRAMP)*
- *New York Department of Financial Services (NY DFS) 23 NYCCRR 500*
- *North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)*

CONTRACTUAL REQUIREMENTS

[fill-in applicable contractual requirements]

Example contractual requirements include:

- *ISO/IEC 27001 certification*
- *Payment Card Industry Data Security Standard (PCI DSS)*
- *Generally Accepted Privacy Principles (GAPP)*
- *American Institute of CPAs Service Organization Control (AICPA SOC2)*
- *Center for Internet Security Critical Security Controls (CIS CSC)*
- *Cloud Security Alliance Cloud Controls Matrix (CSA CCM)*

MANAGEMENT CONTROLS

Management controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity topics. These cybersecurity controls address broader Information Security Management System (ISMS)-level governance of the security program that impact operational, technical and privacy controls.

PROGRAM MANAGEMENT (PM)

P-PM-1: INFORMATION SECURITY PROGRAM PLAN

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective:[5]

a. Develop and disseminate an organization-wide information security program plan that:
   1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
   2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities and compliance;
   3. Reflects the coordination among organizational entities responsible for information security; and
   4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, other organizations and the Nation;
b. Review and update the organization-wide information security program plan per an organization-defined frequency and following organization-defined events; and
c. Protect the information security program plan from unauthorized disclosure and modification.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001], in conjunction with Privacy Officer/Privacy Compliance Manager [OV-LGA-002], Chief Risk Officer (CRO) [XX-RSK-001], Security Architect [SP-ARC-002] and Systems Security Manager [OV-MGT-001]:

(1) Develops an organization-wide information security governance program to provide complete coverage for all cybersecurity and privacy-related controls needed to address statutory, regulatory and contractual obligations, as well as to address possible threats to data and or assets.
(2) Documents the ACME information security program plan in a single document, the Cybersecurity & Data Protection Program (CDPP).
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(4) If necessary, requests corrective action to address identified deficiencies.
(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, documents the results of corrective action and notes findings.
(7) If necessary, requests additional corrective action to address unremediated deficiencies.

[5] *NIST SP 800-53 Rev 5 control PM-1*

P-PM-2: Information Security Program Leadership Role

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement and maintain an organization-wide information security program.[6]

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Executive Cyber Leadership [OV-EXL-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

(1) Leverages the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CSF)[7] for identifying necessary roles and responsibilities, including the Chief Information Security Officer (CISO).
(2) Utilizes existing HR processes to assign formal roles and responsibilities to the CISO to perform or delegate the following cybersecurity management responsibilities:
    a. Establish, document and distribute security policies and procedures;
    b. Monitor and analyze security alerts and information;
    c. Distribute and escalate security alerts to appropriate personnel;
    d. Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
    e. Administer user accounts, including additions, deletions and modifications; and
    f. Monitor and control all access to data.
(3) Provides written notification to the employee assigned the role of CISO.
(4) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(5) If necessary, requests corrective action to address identified deficiencies.
(6) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(7) If necessary, documents the results of corrective action and notes findings.
(8) If necessary, requests additional corrective action to address unremediated deficiencies.

P-PM-3: Information Security and Privacy Resources

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?

[6] *NIST SP 800-53 Rev 5 control PM-2*
[7] *NIST NICE - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework*

ASSESSMENT, AUTHORIZATION & MONITORING (CA)

P-CA-1: ASSESSMENT, AUTHORIZATION & MONITORING POLICY & PROCEDURES

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective:[46]

a. Develop, document and disseminate to organization-defined personnel or roles:
   1. Organization-level assessment, authorization and monitoring policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines; and
   2. Procedures to facilitate the implementation of the assessment, authorization and monitoring policy and the associated assessment, authorization and monitoring controls;
b. Designate an organization-defined official to manage the development, documentation and dissemination of the assessment, authorization and monitoring policy and procedures; and
c. Review and update the current assessment, authorization and monitoring:
   1. Policy per an organization-defined frequency and following organization-defined events; and
   2. Procedures per an organization-defined frequency and following organization-defined events.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001], in conjunction with Privacy Officer/Privacy Compliance Manager [OV-LGA-002], Chief Risk Officer (CRO) [XX-RSK-001], Security Architect [SP-ARC-002] and Systems Security Manager [OV-MGT-001]:

(1) Develops an organization-wide secure engineer practices program that leverages ACME-adopted cybersecurity and privacy principles.
(2) Documents an assessment, authorization & monitoring policy and standards in a single document, the Cybersecurity & Data Protection Program (CDPP).
(3) Requires data/process owners and asset custodians to:
   a. Document function-specific procedures in a Cybersecurity Standardized Operating Procedures (CSOP), or similar format;
   b. Identify applicable statutory, regulatory and contractual obligations (see CDPP Applicability Matrix); and
   c. Include the identification and assignment of roles and responsibilities among internal and external stakeholders.
(4) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
   a. Distributes copies of the change to key personnel; and
   b. Communicates the changes and updates to key personnel.
(5) If necessary, requests corrective action to address identified deficiencies.
(6) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(7) If necessary, documents the results of corrective action and notes findings.
(8) If necessary, requests additional corrective action to address unremediated deficiencies.

[46] *NIST SP 800-53 Rev 5 control CA-1*

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Asset Owner [XX-AST-001], Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

(1) Implements appropriate administrative and technical means to conducts periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team. [239]
(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(3) If necessary, requests corrective action to address identified deficiencies.
(4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(5) If necessary, documents the results of corrective action and notes findings.
(6) If necessary, requests additional corrective action to address unremediated deficiencies.

P-IR-3(2): Incident Response Testing | Coordination with Related Plans

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: Coordinate incident response testing with organizational elements responsible for related plans. [240]

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Asset Owner [XX-AST-001], Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

(1) Implements appropriate administrative means to ensure identify key personnel associated with related plans (e.g., Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), etc.).
(2) Coordinates incident response testing with appropriate personnel responsible for related plans.
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(4) If necessary, requests corrective action to address identified deficiencies.
(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, documents the results of corrective action and notes findings.
(7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-IR-4: Incident Handling

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks

[239] *NIST SP 800-171A assessment criteria 3.6.3*
[240] *NIST SP 800-53 Rev 5 control IR-3(2)*

- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective:[241]

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication and recovery;
b. Coordinate incident handling activities with contingency planning activities;
c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training and testing and implement the resulting changes accordingly; and
d. Ensure the rigor, intensity, scope and results of incident handling activities are comparable and predictable across the organization.

Procedure / Control Activity: Cyber Defense Incident Responder [PR-CIR-001], in conjunction with Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

(1) Leverages ACME's Integrated Incident Response Program (IIRP) to: [242]
    a. Investigate notifications from detection systems;
    b. Identify and assess the severity and classification of incidents;
    c. Define appropriate user response activities to take in response to the incident, in accordance with ACME's Incident Response Plan (IRP); [243]
    d. Respond with appropriate remediation actions to minimize impact and ensure the continuation of business functions; and
    e. As necessary, update the IRP, based on lessons learned from the incident.
(2) Ensures the IIRP includes:
    a. Preparation; [244]
    b. Detection;[245]
    c. Analysis;[246]
    d. Containment;[247] and
    e. Recovery.[248]
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(4) If necessary, requests corrective action to address identified deficiencies.
(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, documents the results of corrective action and notes findings.
(7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-IR-4(1): INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks

[241] *NIST SP 800-53 Rev 5 control IR-4*
[242] *NIST SP 800-171A assessment criteria 3.6.1[a]*
[243] *NIST SP 800-171A assessment criteria 3.6.1[g]*
[244] *NIST SP 800-171A assessment criteria 3.6.1[b]*
[245] *NIST SP 800-171A assessment criteria 3.6.1[c]*
[246] *NIST SP 800-171A assessment criteria 3.6.1[d]*
[247] *NIST SP 800-171A assessment criteria 3.6.1[e]*
[248] *NIST SP 800-171A assessment criteria 3.6.1[f]*

- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: Support the incident handling process using automated mechanisms.[249]

Procedure / Control Activity: Cyber Defense Incident Responder [PR-CIR-001], in conjunction with Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to employ automated mechanisms to support the incident handling process. Automated mechanisms supporting incident handling processes include, for example, online incident management systems.
(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(3) If necessary, requests corrective action to address identified deficiencies.
(4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(5) If necessary, documents the results of corrective action and notes findings.
(6) If necessary, requests additional corrective action to address unremediated deficiencies.

P-IR-4(2): INCIDENT HANDLING | DYNAMIC RECONFIGURATION

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: Include organization-defined types of dynamic reconfiguration for organization-defined system components as part of the incident response capability.[250]

Procedure / Control Activity: System Administrator [OM-ADM-001], in conjunction with Asset Owner [XX-AST-001], Crisis Management Specialist [XX-CON-001], Disaster Recovery Team Leader [XX-CON-003] and Business Continuity Team Leader [XX-CON-005]:

(1) Develops specific use cases where dynamic reconfiguration is appropriate that includes:
    a. Stopping an active attack;
    b. Misdirecting attackers; and
    c. Isolating systems, thus limiting the extent of the damage from breaches or compromises.
(2) Implements appropriate administrative and technical means to employ automated mechanisms that enable dynamic reconfiguration of systems as part of incident response remediation actions that includes:
    a. Changes to router or firewall Access Control Lists (ACLs); and

[249] *NIST SP 800-53 Rev 5 control IR-4(1)*
[250] *NIST SP 800-53 Rev 5 control IR-4(2)*

b. Intrusion Detection / Prevention System (IDS/IPS) parameters.

(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
   a. Distributes copies of the change to key personnel; and
   b. Communicates the changes and updates to key personnel.

(4) If necessary, requests corrective action to address identified deficiencies.

(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.

(6) If necessary, documents the results of corrective action and notes findings.

(7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-IR-4(3): INCIDENT HANDLING | CONTINUITY OF OPERATIONS

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: Identify classes of incidents and take organization-defined actions in response to those incidents to ensure continuation of organizational mission and business functions.[251]

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Systems Security Analyst [OM-ANA-001], Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-02 and Cyber Defense Incident Responder [PR-CIR-001]:

(1) Leverages the Integrated Incident Response Program (IIRP) to categorize cybersecurity incidents based on each category's potential to escalate and different handling procedures:

#	Threat	Category	Category Description
0	Training	**Simulated Incident** (Training & Exercises)	This category is used during exercises and approved testing of internal/external network defenses or responses.
1	Illegal Content or Activities	**Illegal Content**	This category is used for any data that is illegal to have in possession. This includes illegal content such as child pornography or classified information on unclassified systems.
2		**Criminal Conduct**	This category is used for any incident that would be considered criminal conduct. This includes embezzlement, corporate espionage, terrorism/national security threats, fraud, violence or other conduct that would constitute a criminal felony or misdemeanor charge.
3	Safety	**Technology Compromise**	This category is used for any incident that has safety implications from the compromise of the technology to be used in a manner it was not designed for. This includes categories of technologies that includes Operational Technology (OT) and Internet of Things (IoT).

[251] *NIST SP 800-53 Rev 5 control IR-4(3)*

4	**Confidentiality**	**Breach of Sensitive Data**	This category is used for any incident that has involves the unauthorized disclosure or compromise of sensitive data. This includes sensitive Personal Data (PD) and Intellectual Property (IP).
5	**Nefarious Activity**	**Malware**	This category is used for malware-related incidents. Any software code intentionally created or introduced into multiple systems for the distinct purpose of causing hard or loss to the computer system, its data or other resources (e.g., spyware, adware, viruses, Trojans, worms, etc.).
6		**Host / Application Compromise**	This is a known or suspected compromise that is not directly related to malware. A successful event of this nature means the attacker has total control over the host or application and access to any and all data stored on it or on systems that trust the compromised host or application. This may be from a privilege escalation attack.
7		**Denial of Service (DoS)**	This is a known or suspected Denial of Service (DoS) attack. A successful event of this nature means the attacker(s) successfully denied access to either the entire network, a portion of the network or to critical service(s) / website(s).
8	**Lost / Stolen Asset**	**Lost / Stolen IT Asset**	This category is used to respond to any lost or stolen IT equipment (e.g., laptops, tablets, computers, servers, media, tapes, etc.)
9	**Poor Security Practice**	**Poor Security Practice**	This category is used for any suspected incident involving misconfigurations, poor cybersecurity practices & policy violations.
10	**Unknown / Other**	**Unknown / Other** (Under Investigation)	This category is used if the situation is unclear and categorization cannot be made. This is meant to be a "placeholder" category until the threat or situation is investigated and a final determination has been made, so that the incident can be properly categorized.

(2) Implements appropriate administrative and technical means to employ the IIRP to ensure users understand the different categories of incidents and the actions required to be taken, per ACME's Incident Response Plan (IRP).

(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:

a. Distributes copies of the change to key personnel; and

b. Communicates the changes and updates to key personnel.

(4) If necessary, requests corrective action to address identified deficiencies.

(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.

(6) If necessary, documents the results of corrective action and notes findings.

(7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-IR-4(4): Incident Handling | Information Correlation

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?