Your Logo
Will Be
Placed Here

STANDARDIZED OPERATING PROCEDURES (SOP)

ACME Business Consulting, Inc.

EXAMPLE

SCF SECURE CONTROLS FRAMEWORK

CSOP
Cybersecurity Standardized Operating Procedures

INTERNAL USE
Access Limited to Internal Use Only

IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)

Table of Contents

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

EXAMPLE

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.

EXAMPLE

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.

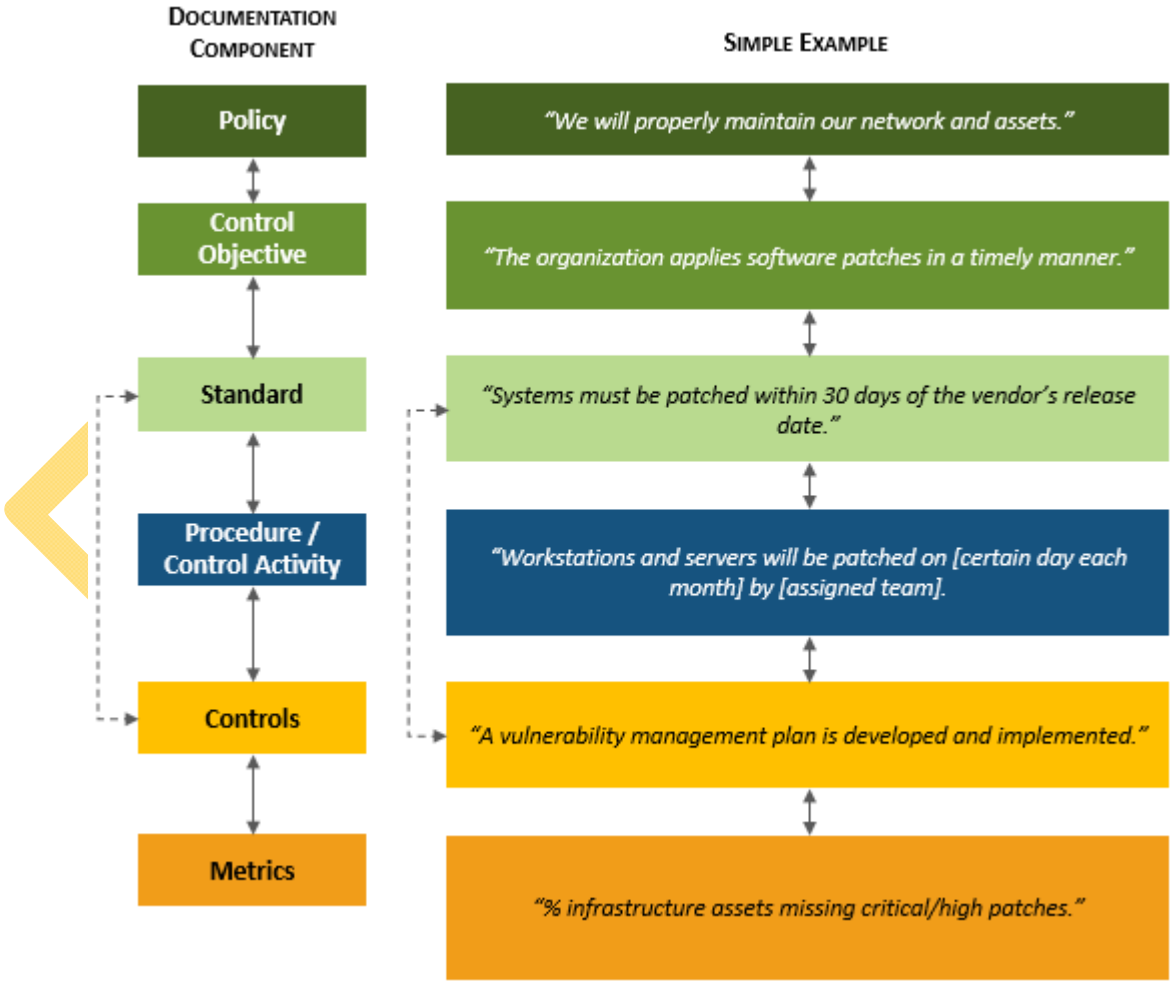
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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

This example is a configuration procedure **P-CFG-02 (System Hardening Through 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: Mechanisms exist to develop, document and maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards. *[control wording comes directly from the Secure Controls Framework (SCF) control #CFG-02. The SCF is a free resource that can be downloaded from https://www.securecontrolsframework.com]*

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 that enable the implementation of appropriate physical, administrative and technical mechanisms to ensure baseline system hardening configuration for all ACME-owned or managed assets comply with applicable legal, statutory, and regulatory compliance obligations.
(2) Where technically feasible, technology platforms align with industry-recommended hardening recommendations, including but not limited to:
    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
    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;

EXAMPLE

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 2nd 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.

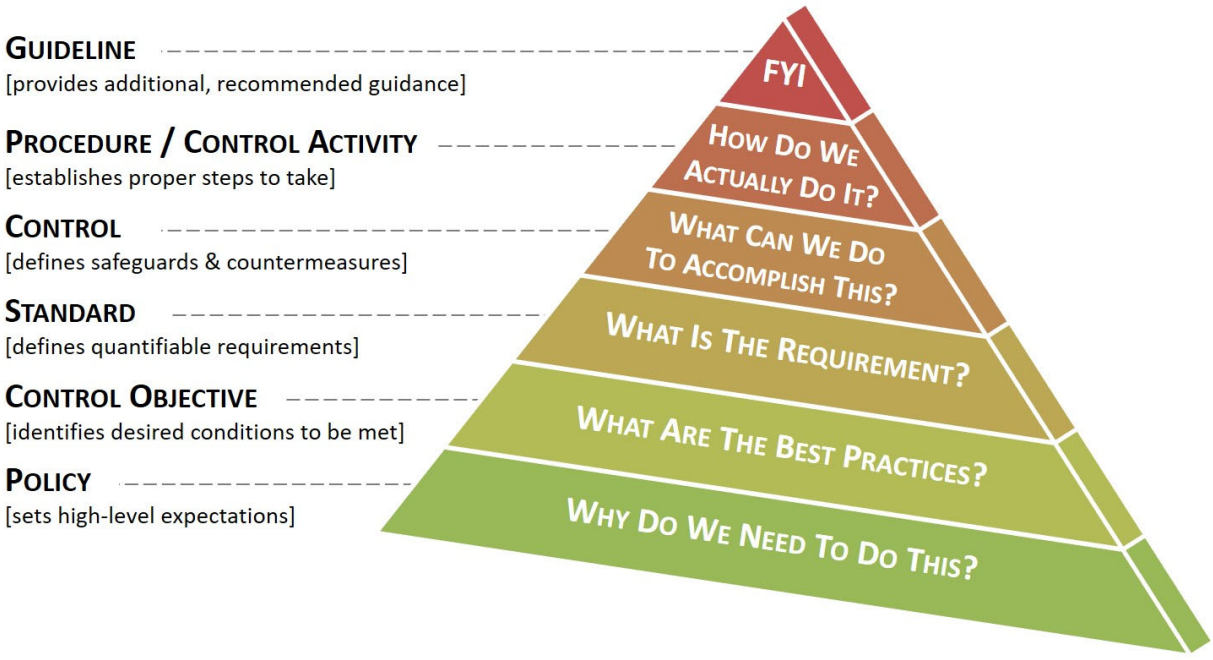
EXAMPLE

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 Digital Security Program (DSP) that contains policies, control objectives, standards and guidelines. It also directly maps to the Secure Controls Framework (SCF) for cybersecurity and privacy controls.

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

EXA

P-GOV-08: Defined Business Context & Mission

Control: Mechanisms exist to define the context of its business model and document the mission of the organization.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001], in conjunction with Systems Security Manager [OV-MGT-001]:

(1) Researches, establishes and documents:
    a. ACME's business model.
    b. ACME's corporate mission statement so that cybersecurity-related objectives can be tied back to strategic concerns.
    c. Strength, Weakness, Opportunities & Threats (SWOT) analysis to define external and internal issues that are relevant and that affect the organization's ability to achieve ACME's mission (e.g., industry drivers, relevant regulations, basis for competition, etc.).
(2) Prioritizes the objectives and activities necessary to support ACME's corporate mission in a cybersecurity and privacy-specific business plan that takes a multi-year approach to documenting:
    a. Current maturity capability levels associated with cybersecurity and privacy-related People, Processes and Technologies (PPT).
    b. Target maturity capability levels associated with cybersecurity and privacy-related PPT.
    c. Resource requirements.
    d. Cybersecurity and privacy specific:
        i. Vision.
        ii. Mission.
        iii. Strategy.
    e. Prioritized objectives to accomplish the business plan.
(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-GOV-09: Defined Control Objectives

Control: Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001], in conjunction with Systems Security Manager [OV-MGT-001]:

(1) Researches, establishes and documents the appropriate internal control system for both cybersecurity and privacy controls that supports ACME's applicable statutory, regulatory and/or contractual obligations.
(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.

EXAMPLE

P-MON-06(B): MONITORING REPORTING | TREND ANALYSIS REPORTING

Control: Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Procedure / Control Activity: Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Security Architect [SP-ARC-002] and Executive Cyber Leadership [OV-EXL-001]:

(1) Develop measures of performance or outcome-based metrics, to enable trend analysis through measuring the effectiveness or efficiency of the cybersecurity program and the security controls employed in support of the program that incorporates:
    a. Recent threat information regarding the types of threat events that have occurred within the organization or across the federal government;
    b. Success rates of certain types of cyber attacks;
    c. Emerging vulnerabilities in information technologies;
    d. Evolving social engineering techniques;
    e. Results from multiple security control assessments;
    f. The effectiveness of configuration settings; and
    g. Findings from Internal Audit (IA) or third-party assessors.
(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-MON-07: TIME STAMPS

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) 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: Mechanisms exist to configure systems to use internal system clocks to generate time stamps for audit records.

Procedure / Control Activity: System Administrator [OM-ADM-001], in conjunction with Systems Security Analyst [OM-ANA-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time.
(2) Enables NTP for client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.[7]
(3) Utilizes The official NIST or USNO Internet Time Service (ITS) for system time synchronization:
    a. time.nist.gov 192.43.244.18 [primary].

[7] http://tycho.usno.navy.mil/ntp.html

b. time-nw.nist.gov 131.107.13.100 [alternate].

(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-MON-07(A): TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) 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: Mechanisms exist to synchronize internal system clocks with an authoritative time source.

Procedure / Control Activity: System Administrator [OM-ADM-001], in conjunction with Systems Security Analyst [OM-ANA-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time.
(2) Enables NTP is the Internet standard protocol for client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.[8]
(3) Utilizes The official NIST or USNO Internet Time Service (ITS) for system time synchronization:
   a. time.nist.gov 192.43.244.18 [primary].
   b. time-nw.nist.gov 131.107.13.100 [alternate].
(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-MON-08: PROTECTION OF AUDIT INFORMATION

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) 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

[8] http://tycho.usno.navy.mil/ntp.html

P-HRS-13: Identify Critical Skills & Gaps

Control: Mechanisms exist to evaluate the critical cybersecurity and privacy skills needed to support the organization's mission and identify gaps that exist.

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

(1) Conducts a critical skills inventory that:
    a. Analyzes the appropriate skills that are required to support the organization's mission and business functions;
    b. Documents competencies necessary to define critical skills;
    c. Inventories the current technology staff for the identified critical skills;
    d. Documents the gap that exists in current versus needed critical skills;
    e. Proposes a solution to address the critical skills shortfall.
(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-HRS-13(a): Identify Critical Skills & Gaps | Remediate Identified Skills Deficiencies

Control: Mechanisms exist to remediate critical skills deficiencies necessary to support the organization's mission and business functions.

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

(1) Remediate critical skills deficiencies by:
    a. Resourcing new hires;
    b. Outsourcing the responsibilities to a competent third-party;
    c. Reassigning and training existing staff; and/or
    d. Creating new positions with higher level skill requirements.
(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-HRS-13(b): Identify Critical Skills & Gaps | Identify Vital Cybersecurity & Privacy Staff

Control: Mechanisms exist to identify vital cybersecurity & privacy staff.

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

(1) Identifies the objectives and activities necessary to support ACME's corporate mission:
    a. Current maturity capability levels associated with cybersecurity and privacy-related People, Processes and Technologies (PPT).
    b. Target maturity capability levels associated with cybersecurity and privacy-related PPT.
    c. Resource requirements.
    d. Cybersecurity and privacy specific:
        i. Vision.
        ii. Mission.
        iii. Strategy.

EXAMPLE

e. Prioritized objectives to accomplish the business plan.

(2) Identifies critical staff by:
   a. Identifying vital cybersecurity & privacy staff;
   b. Documenting the role, function, responsibility and reasons that supports their designation as vital;
   c. Where possible, identifying staff that can backfill vital roles.
(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-HRS-13(c): Identify Critical Skills & Gaps | Establish Redundancy for Vital Cybersecurity & Privacy Staff

Control: Mechanisms exist to establish redundancy for vital cybersecurity & privacy staff.

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

(1) Conducts a critical skills inventory that:
   a. Analyzes the appropriate skills that are required to support the organization's mission and business functions;
   b. Documents competencies necessary to define critical skills;
   c. Inventories the current technology staff for the identified critical skills;
   d. Documents the gap that exists in current versus needed critical skills;
(2) Designates roles that require redundancy.
(3) Identifies a primary and alternate staff member for vital cybersecurity & privacy roles.
(4) Proposes a solution to address any redundancy shortfalls.
(5) 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.
(6) If necessary, requests corrective action to address identified deficiencies.
(7) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(8) If necessary, documents the results of corrective action and notes findings.
(9) If necessary, requests additional corrective action to address unremediated deficiencies.

P-HRS-13(d): Identify Critical Skills & Gaps | Perform Succession Planning

Control: Mechanisms exist to perform succession planning for vital cybersecurity & privacy roles.

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

(1) Manages succession planning as an extensive and systematic activity that:
   a. Maintains documented roles and responsibilities for vital cybersecurity & privacy staff positions;
   b. Works with senior leaders who responsible those vital cybersecurity & privacy staff positions to develop succession plans;
   c. Works with identified staff members to provide training and/or guidance on steps needed to successfully move into the new role if succession plans must be implemented to help ensure a smooth transition.
(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.

EXAMPLE

P-IRO-02(c): Incident Handling | Dynamic Reconfiguration

Control: Automated mechanisms exist to dynamically reconfigure information system components as part of the incident response capability.

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) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to implement appropriate administrative and technical mechanisms 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);
    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-IRO-02(d): Incident Handling | Continuity of Operations

Control: Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.

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).

SAMPLE

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) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to implement appropriate administrative and technical mechanisms 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.

EXAMPLE

P-PES-03(C): PHYSICAL ACCESS CONTROL | PHYSICAL ACCESS LOGS

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) 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: Physical access control mechanisms exist to generate a log entry for each access through controlled ingress and egress points.

Procedure / Control Activity: Physical Security Specialist [XX-PES-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure access control systems to log the following information:
    a. Physical location of the access;
    b. Direction of access, if possible (e.g., ingress or egress);
    c. Identity of the person accessing the location; and
    d. Indication of success or failure.
(2) Uses a visitor log to maintain a physical audit trail of visitor activity:
    a. At a minimum, document the visitor's name, the company represented, and the onsite personnel authorizing physical access; and
    b. Retain this log for a minimum of three months, unless otherwise restricted by law.
(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-PES-03(D): PHYSICAL ACCESS CONTROL | ACCESS TO INFORMATION SYSTEMS

Control: Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive data, in addition to the physical access controls for the facility.

Procedure / Control Activity: Asset Owner [XX-AST-001], in conjunction with Physical Security Specialist [XX-PES-001] and Physical Security Manager [XX-PES-002]:

(1) Implements appropriate administrative, physical and technical means to enforce physical access authorizations to information systems in addition to the physical access controls.
(2) Develops unique physical security zones to determine specific areas that are more vulnerable to unauthorized use, theft or viewing of data where enhanced physical safeguards should be implemented:
    a. Facilities management implements physical access authorization mechanisms to secure workspaces, such as:
        i. Proximity badges; or
        ii. Personalized PIN pad
    b. Line supervisors and manage facilitate "clean desk" requirements for all work areas to ensure media containing sensitive data is properly secured when the workspace is not occupied, including:
        i. Filing cabinets, lockable drawers / overhead cabinets, storage rooms and any other storage unit containing sensitive data will be locked when not in use; and

EXAMPLE