YOUR LOGO GOES HERE

NIST SP 800-171 & CMMC
CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

ACME Professional Services, LLC

CSOP
Cybersecurity Standardized
Operating Procedures

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

Table of Contents

Identification & Authentication (IAC) Procedures 68

Incident Response (IRO) Procedures 85

Information Assurance (IAO) Procedures 90

Maintenance (MNT) Procedures 95

Overview, Instructions & 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.

?
Remaining Customization ~ 20%
Procedure Statements
~80% Complete

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.

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 cybersecurity program, since procedures represents the specific activities that are performed to protect systems and data.

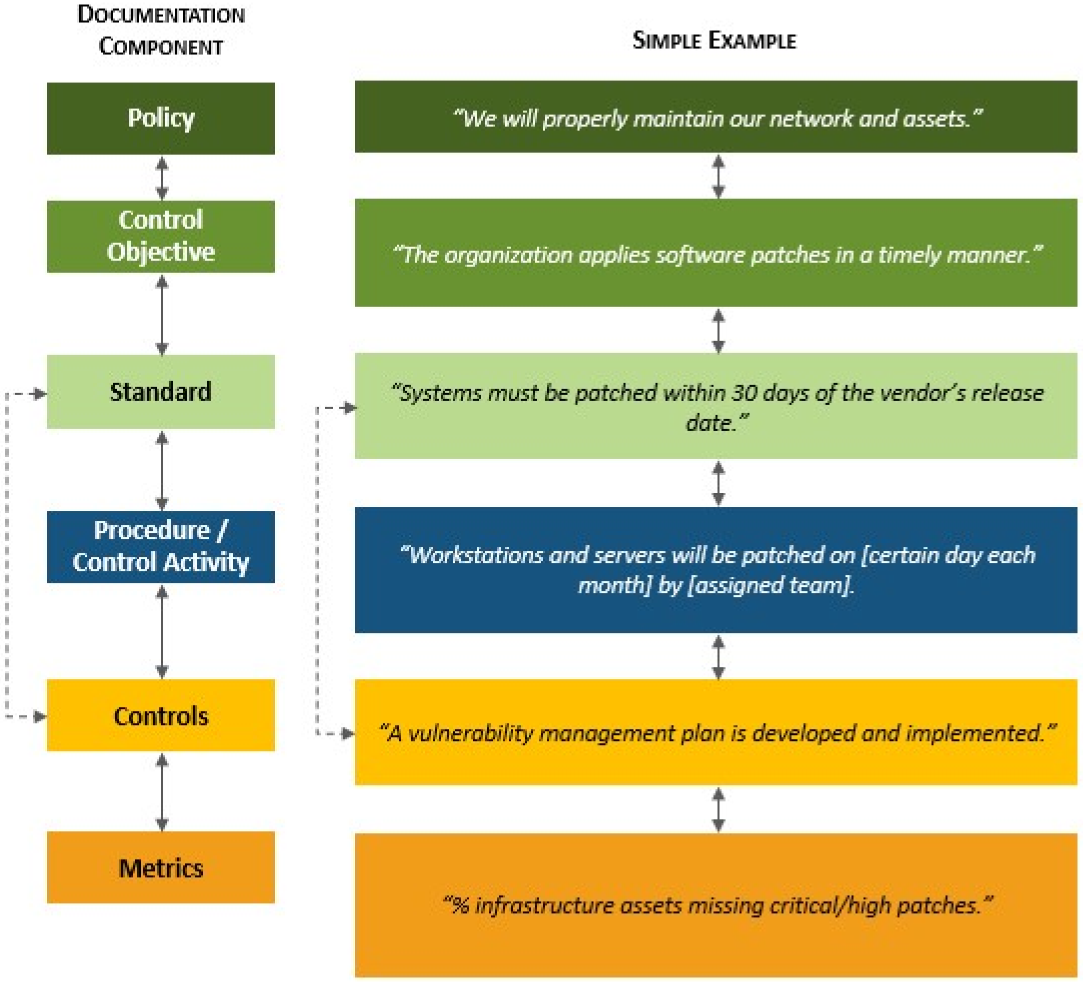
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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.



"We will properly maintain our network and assets."

"The organization applies software patches in a timely manner."

"Systems must be patched within 30 days of the vendor's release date."

"Workstations and servers will be patched on [certain day each month] by [assigned team]."

"A vulnerability management plan is developed and implemented."

"% infrastructure assets missing critical/high patches."

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!

OVERSEE & GOVERN	OPERATE & MAINTAIN	INVESTIGATE	COLLECT & OPERATE	ANALYZE	SECURELY PROVISION	PROTECT & DEFEND

NIST NICE Cybersecurity Workforce Framework – Work Categories

Example Procedure Statement

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;

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.

ASSET MANAGEMENT (AST) PROCEDURES

Management Intent: The purpose of the Asset Management (AST) procedures / control activities is to ensure that technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal.

P-AST-01: ASSET GOVERNANCE

Control: Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.

Procedure / Control Activity: IT Asset Management (ITAM) Manager [XX-AST-002], in conjunction with Asset Owner [XX-AST-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to maintain current inventories of ACME's technology assets that includes, but is not limited to:

  a. A list of all such devices and personnel with access;

  b. A method to accurately and readily determine owner, contact information, and purpose (e.g., labeling, coding, and/or inventorying of devices); and

  c. A list of company-approved products.

(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, IT Asset Management (ITAM) Manager [XX-AST-002], in conjunction with Asset Owner [XX-AST-001], 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-AST-02: ASSET INVENTORIES

Control: Mechanisms exist to perform inventories of technology assets that:

- Accurately reflects the current systems, applications and services in use;
- Identifies authorized software products, including business justification details;
- Is at the level of granularity deemed necessary for tracking and reporting;
- Includes organization-defined information deemed necessary to achieve effective property accountability; and
- Is available for review and audit by designated organizational personnel.

Procedure / Control Activity: Asset Owner [XX-AST-001], in conjunction with System Administrator [OM-ADM-001]:

(1) Maintains an inventory of technology assets that includes, but is not limited to: [2]

  a. Hardware and software inventories, both:

    i. Internally-hosted assets; and

    ii. Externally-hosted assets; and

  b. A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding, and/or inventorying of devices).

(2) Assigns one of the following classifications to each technology asset, per CMMC scoping guidelines:

  a. CUI Asset;

  b. Security Protection Asset (SPA);

  c. Contractor Risk Managed Asset (CRMA)

  d. Specialized Asset (SA); or

  e. Out of Scope Asset (OSA);

(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, updates the inventory.

(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.

[2] *NIST SP 800-171A / CMMC assessment criteria 3.4.1[d], 3.4.1[e] & 3.4.1[f] / CM.L2-3.4.1[d], CM.L2-3.4.1[e] & CM.L2-3.4.1[f]*

Management Intent: The purpose of the Change Management (CHG) procedures / control activities is for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise.

P-CHG-01: CHANGE MANAGEMENT PROGRAM

Control: Mechanisms exist to facilitate the implementation of a change management program.

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

(1) Develops, implements and governs controls that are sufficient for managing and documenting change management activities that includes:
   a. A formal, documented change management program; and
   b. Processes to facilitate the implementation of changes.
(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-CHG-02: CONFIGURATION CHANGE CONTROL

Control: Mechanisms exist to govern the technical configuration change control processes.

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

(1) Develops, implements and governs controls that are sufficient for managing and documenting change management activities that includes:
   a. A formal, documented change management program; and
   b. Processes to facilitate the implementation of changes, where changes are:
      i. Tracked; [4]
      ii. Reviewed; [5]
      iii. Approved or Disapproved; [6] and
      iv. Documented. [7]
(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.

[4] *NIST SP 800-171A / CMMC assessment criteria 3.4.3[a] / CM.L2-3.4.3[a]*
[5] *NIST SP 800-171A / CMMC assessment criteria 3.4.3[b] / CM.L2-3.4.3[b]*
[6] *NIST SP 800-171A / CMMC assessment criteria 3.4.3[c] / CM.L2-3.4.3[c]*
[7] *NIST SP 800-171A / CMMC assessment criteria 3.4.3[d] / CM.L2-3.4.3[d]*

P-CHG-02.2: Configuration Change Control | Test, Validate & Document Changes

Control: Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.

Procedure / Control Activity: Change Control Manager [XX-CHG-001]:

(1) Implements appropriate administrative and technical means to ensure asset owner and custodians:
a. Test and validate configuration changes in a test environment, prior to deploying the change in the production environment; and
b. Review and test systems, applications and processes to ensure there is no adverse impact on organizational operations or security when major upgrades/updates are applied.

(2) If it is not technically or logistically feasible to test a configuration change, identifies compensating controls to mitigate any negative impact to the production environment from an adverse change event. Compensating controls can include:
a. Images of systems;
b. Backups of configurations;
c. Viable back out plan; and/or
d. After-hours implementation.

(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-CHG-03: Security Impact Analysis for Changes

Control: Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.

Procedure / Control Activity: System Administrator [OM-ADM-001], in conjunction with Asset Owner [XX-AST-001] and Change Control Manager [XX-CHG-001]:

(1) Follows published ACME change control processes to evaluate the security impact for changes that includes:

(2) From a test environment, tests proposed changes specifically to assess the security functions of the system(s) to verify that those functions are:
a. Implemented correctly;
b. Operate as intended; and
c. Meet the security requirements for the system.

(3) Performs a security impact analysis to understand security control requirements and review system design documentation to understand control implementation and how specific changes might affect the controls. The analysis process includes a review of: [8]
a. Separate development/test and production environments;
b. Separation of duties between development/test and production environments;
c. Production data (live data) are not used for testing or development; and
d. Removal of test data and accounts before production systems become active.

(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.

[8] *NIST SP 800-171A / CMMC assessment criteria 3.4.4 / CM.L2-3.4.4[a]*

b. Security tape to identify signs of physical tampering.

(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-CFG-03: Least Functionality

Control: Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.

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 to ensure configuration parameters follow "least functionality" principles to limit privileges to the minimum amount necessary for the user/service to perform needed functions. [18]

(2) Defines essential programs and services. [19]

(3) Defines approved ports, protocols and services. [20]

(4) Identifies non-essential and/or insecure ports, protocols and services. [21]

(5) Enables only necessary and secure services, protocols and daemons, as required for the function of the system. [22]

(6) Implements security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.).

(7) Verifies services, protocols and ports are documented and properly implemented by examining firewall and router configuration settings.

(8) Removes or disables all unnecessary or insecure: [23]

a. Scripts;

b. Drivers;

c. Features;

d. Subsystems;

e. File systems; and

f. Unnecessary web servers.

(9) Utilizes network scanning tools, intrusion detection and prevention systems and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols and services.

(10) 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.

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

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

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

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

P-CFG-03.1: Least Functionality | Periodic Review

Control: Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.

[18] *NIST SP 800-171A / CMMC assessment criteria 3.4.6[a] / CM.L2-3.4.6[a]*

[19] *NIST SP 800-171A / CMMC assessment criteria 3.4.7[a], 3.4.7[d] & 3.4.7[m] / CM.L2-3.4.7[a], CM.L2-3.4.7[d] & CM.L2-3.4.7[m]*

[20] *NIST SP 800-171A / CMMC assessment criteria 3.4.7[g] & 3.4.7[j] / CM.L2-3.4.7[g] & CM.L2-3.4.7[j]*

[21] *NIST SP 800-171A / CMMC assessment criteria 3.4.7[b], 3.4.7[e] & 3.4.7[n] / CM.L2-3.4.7[b], CM.L2-3.4.7[e] & CM.L2-3.4.7[n]*

[22] *NIST SP 800-171A / CMMC assessment criteria 3.4.6[b] / CM.L2-3.4.6[b]*

[23] *NIST SP 800-171A / CMMC assessment criteria 3.4.7[c], 3.4.7[f], 3.4.7[h], 3.4.7[i], 3.4.7[k], 3.4.7[l] & 3.4.7[o] / CM.L2-3.4.7[c], CM.L2-3.4.7[f], CM.L2-3.4.7[h], CM.L2-3.4.7[i], CM.L2-3.4.7[k], CM.L2-3.4.7[l] & CM.L2-3.4.7[o]*

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

1. Performs periodic reviews systems to identify non-secure functions, ports, protocols, and services.
2. Disables unnecessary and non-secure functions, ports, protocols, and services.
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-CFG-03.2: Least Functionality | Prevent Unauthorized Software Execution

Control: Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.

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 to configure systems to employ automated mechanisms that prevent program execution of unauthorized software programs. This includes:
   a. Host Intrusion Prevention System (HIPS) technology;
   b. Advanced antimalware technology; and
   c. Whitelisting / blacklisting applications.

(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-CFG-03.3: Least Functionality | Unauthorized or Authorized Software (Blacklisting or Whitelisting)

Control: Mechanisms exist to whitelist or blacklist applications in an order to limit what is authorized to execute on systems.

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 to configure systems to employ automated mechanisms that prevent program execution of unauthorized software programs through blacklisting/whitelisting applications to: [24]
   a. Identify specific software programs not authorized to execute on the system; [25]
   b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; [26] and
   c. Periodically review and update the list of unauthorized software programs.

(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.

[24] *NIST SP 800-171A / CMMC assessment criteria 3.4.8[a] / CM.L2-3.4.8[a]*

[25] *NIST SP 800-171A / CMMC assessment criteria 3.4.8[b] / CM.L2-3.4.8[b]*

[26] *NIST SP 800-171A / CMMC assessment criteria 3.4.8[c] / CM.L2-3.4.8[c]*