YOUR LOGO GOES HERE

CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

CMMC Level 1 / FAR 52.204-21

ACME Professional Services, LLP

SENSITIVE

Access Limited to Authorized Personnel

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.

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.

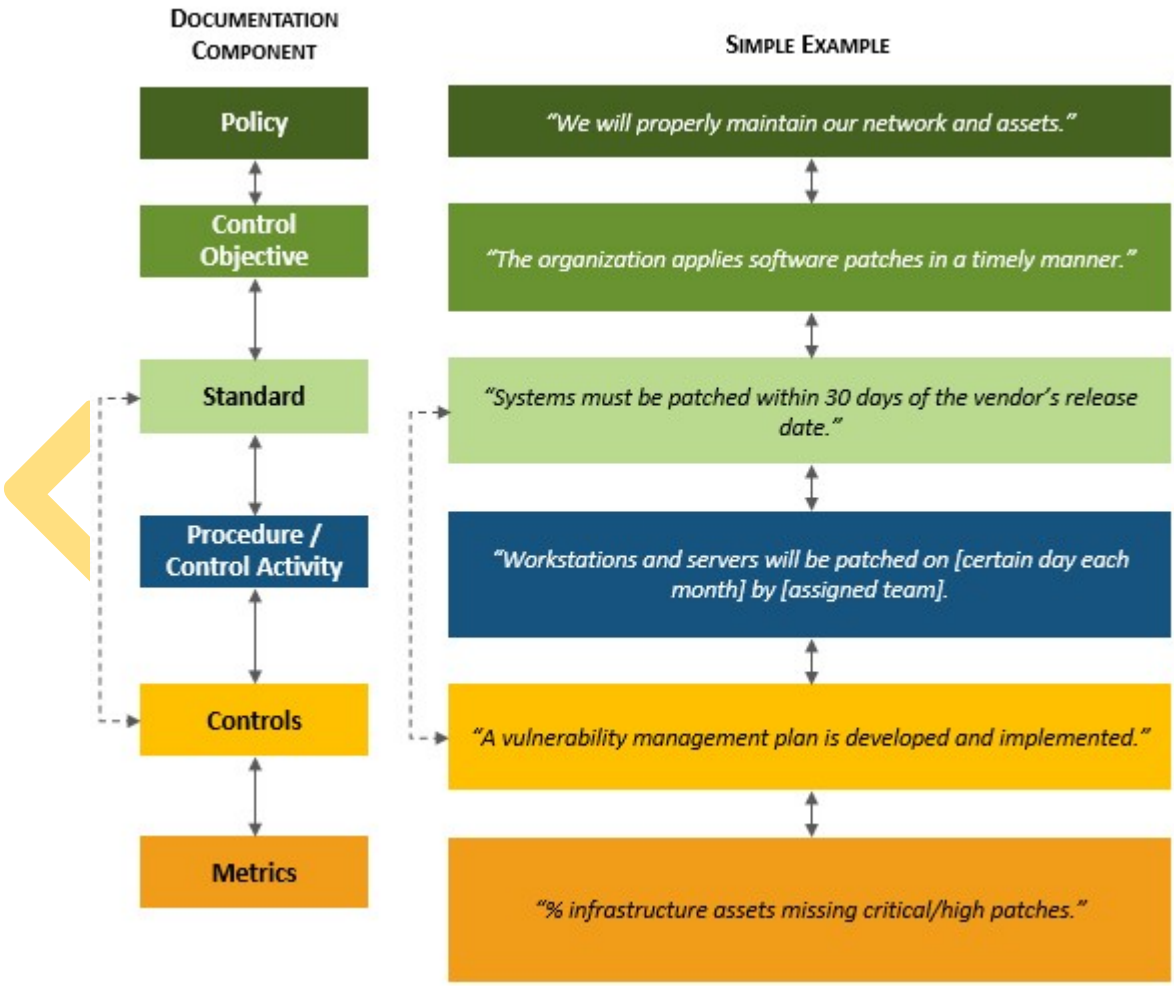
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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

- Certain standards require processes to exist *(due diligence – 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 care – 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.



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 data protection 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 v1.0.0 Cybersecurity Workforce Framework – Work Categories

Example

This example is a configuration procedure **P-CFG-02 (System Hardening Through Baseline Configurations)**

NOTE: THIS PROCESS SECTION CAN BE USED AS A GUIDE TO TAILOR PROCEDURES

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 assigned 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/nice-framework-resource-center*

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 #P-CFG-02. The SCF is a free resource that can be downloaded from https://www.securecontrolsframework.com]*

Procedure / Control Activity: Secure Systems Development [DD-WRL-004], in conjunction with the Technical Support [IO-WRL-007] and Cybersecurity Architecture [DD-WRL-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure baseline system hardening configurations for all ACME-owned or managed assets comply with applicable legal, statutory and regulatory compliance obligations throughout the System Development Life Cycle (SDLC). [2]
    a. Includes hardware, software and firmware in baseline configurations. [3]
    b. Where technically feasible, technology platforms align with reasonably-expected hardening practices that apply the appropriate use of common security configurations available from the National Institute of Standards and Technology's National Checklist Program (NCP) website:[4]
        i. Center for Internet Security (CIS) benchmarks;[5]
        ii. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs); [6]or
        iii. Original Equipment Manufacturer (OEM) security configuration guidance.

(2) Technology platforms that include, but are not limited to:
    a. Server-Class Systems
        i. Microsoft Server 2016
        ii. Microsoft Server 2018
        iii. Microsoft Server 2020
        iv. Microsoft Server 2022
        v. Red Hat Enterprise Linux (RHEL)
        vi. Unix
        vii. Solaris
    b. Workstation-Class Systems
        i. Microsoft 10
        ii. Microsoft 11
        iii. Apple
        iv. Fedora (Linux)
        v. Ubuntu (Linux)
        vi. SuSe (Linux)
    c. Network Devices
        i. Firewalls
        ii. Routers
        iii. Load balancers
        iv. Virtual Private Network (VPN) concentrators
        v. Wireless Access Points (WAPs)
        vi. Wireless controllers
        vii. Printers
        viii. Multi-Function Devices (MFDs)
    d. Mobile Devices
        i. Tablets
        ii. Mobile phones
        iii. Other portable electronic devices
    e. Databases
        i. MySQL

---

[2] *NIST SP 800-171A / CMMC 2.0: 3.4.1[a], 3.4.1[c], 3.4.2[a] & 3.4.2[b] / CM.L2-3.4.1[a], CM.L2-3.4.1[c], CM.L2-3.4.2[a] & CM.L2-3.4.2[b]*

[3] *NIST SP 800-171A / CMMC 2.0: 3.4.1[b] / CM.L2-3.4.1[b] | NIST SP 800-171A R3: A.03.01.03[01], A.03.01.16.a[03], A.03.01.16.c, A.03.01.18.a[02], A.03.03.08.a[02], A.03.04.01.a[01], A.03.04.01.a[02], A.03.04.02.a[01], A.03.04.02.a[02], A.03.04.06.b[01], A.03.04.06.b[02], A.03.04.06.b[03], A.03.04.06.b[04], A.03.04.06.b[05], A.03.04.06.ODP[01], A.03.04.06.ODP[02], A.03.04.06.ODP[03], A.03.04.06.ODP[04], A.03.04.06.ODP[05], A.03.05.04[01], A.03.05.04[02], A.03.05.07.c, A.03.05.07.d, A.03.05.07.e, A.03.05.07.f, A.03.07.05.b[02]*

[4] *NIST NCP website - https://ncp.nist.gov/repository*

[5] *CIS Benchmarks - https://www.cisecurity.org/cis-benchmarks/*

[6] *DISA STIGs official site - https://public.cyber.mil/stigs/*

ii. Windows SQL Server
iii. Windows SQL Express
iv. Oracle
v. DB2

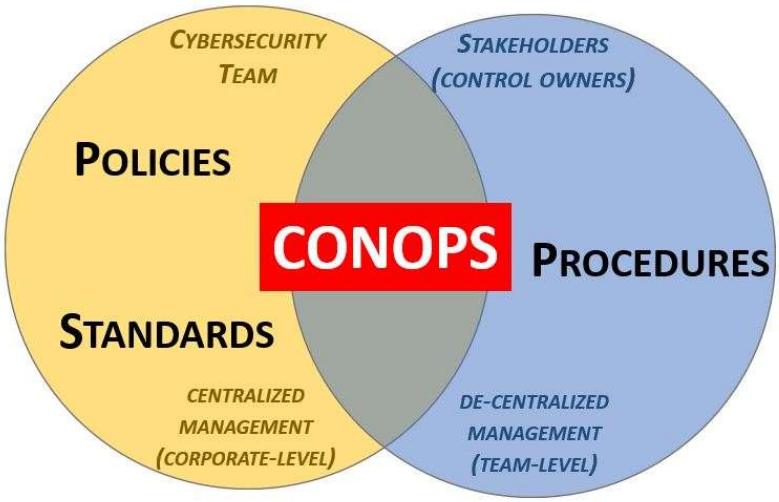
(3) Ensures that system hardening includes, but is not limited to the following criteria:
   a. Each Operating System (OS) must:
      i. Be hardened to provide only necessary functionality (e.g., ports, protocols, services, etc.) to meet business needs;
      ii. Prevent remote devices from simultaneously establishing nonremote connections with organizational systems and communicating via some other unauthorized connection to resources in external networks (e.g., split tunneling); and
      iii. Include necessary technology controls that are required for the secure use of the OS in a production environment (e.g., antimalware, event log forwarding, content filtering, etc.);
   b. Deviations from secure baseline configurations must be:
      i. Approved in accordance with ACME's change management processes, prior to deployment, provisioning or use;[7] and
      ii. Authorized following change management processes prior to deployment, provisioning or use.
   c. 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.
   d. Configuring and documenting only the necessary ports, protocols and services to meet business needs;
   e. 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;
   f. 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
   g. 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) 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.
(6) 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.
(7) If necessary, requests corrective action to address identified deficiencies.
(8) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(9) If necessary, documents the results of corrective action and notes findings.
(10) If necessary, requests additional corrective action to address unremediated deficiencies.

[7] *NIST SP 800-171A R3: A.03.04.02.b[01], A.03.04.02.b[02]*

Supporting Policies & Standards

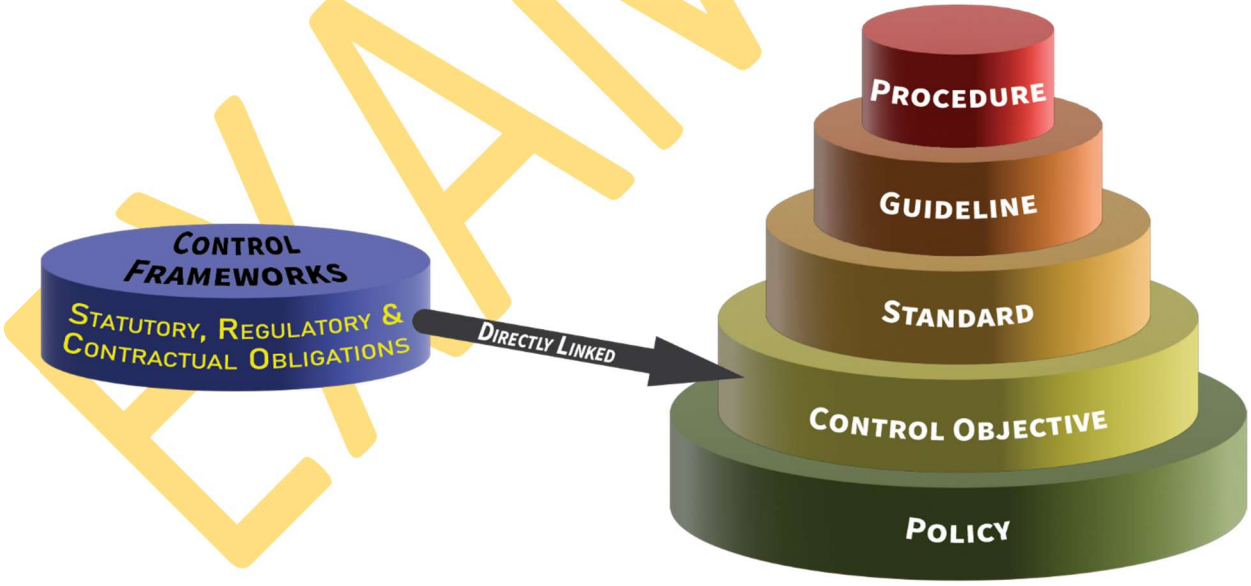
While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with Cybersecurity & Data Protection Program (CDPP) that contains policies, control objectives, standards and guidelines.



Policies, Controls, Standards, Procedures & Guidelines Structure

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

(1) Policy that establishes management's intent;
(2) Control Objective that identifies leading practices (linked to controls);
(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.



Management Intent: The purpose of the Cybersecurity & Data Protection Governance (GOV) procedures / control activities is to specify the development, proactive management and ongoing review of ACME's cybersecurity and data protection program.

P-GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM

Control: Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.

Procedure / Control Activity: Systems Security Management [OG-WRL-014], in conjunction with Cybersecurity Architecture [DD-WRL-001] and Executive Cybersecurity Leadership [OG-WRL-007]:

(1) Develops an organization-wide cybersecurity and data protection governance program to provide complete coverage for all cybersecurity and data protection-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 cybersecurity and data protection governance program 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.

P-GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION

Control: Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.

Procedure / Control Activity: Cybersecurity Policy and Planning [OG-WRL-002], in conjunction with Executive Cybersecurity Leadership [OG-WRL-007], Systems Security Management [OG-WRL-014] and Cybersecurity Legal Advice [OG-WRL-006]:

(1) Analyzes all applicable statutory, regulatory and contractual obligations to create a list of requirements that need to be addressed by ACME's policies and standards.
(2) Analyzes the most current risk assessment(s) to determine appropriate coverage for ACME's specific capabilities, based on people, processes and technology resources.
(3) Designs and documents ACME's cybersecurity and data protection policies and standards in a consolidated document, the Cybersecurity & Data Protection Program (CDPP).[8]
(4) Directs asset / process owners (e.g., control owners) to:
    a. Design and document business process and technology-specific procedures that describe how applicable cybersecurity and data protection controls are operationalized;[9] and
    b. Disseminate procedures with all applicable stakeholders.[10]
(5) Receives written endorsement from executive management.
(6) Disseminates the DSP to all affected parties to ensure all ACME personnel understand their applicable requirements.[11]
(7) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, or as business/technology changes require modifications, reviews and updates to the DSP, to ensure proper coverage for applicable statutory, regulatory and contractual requirements;
(8) Whenever the DSP is updated:

[8] *NIST SP 800-171A R3: A.03.15.01.a[01]*
[9] *NIST SP 800-171A R3: A.03.15.01.a[03]*
[10] *NIST SP 800-171A R3: A.03.15.01.a[04]*
[11] *NIST SP 800-171A R3: A.03.15.01.a[02]*

Management Intent: The purpose of the Asset Management (AST) procedures / control activities is to ensure that Technology Assets, Applications and/or Services (TAAS) 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 [IO-ORG-001], in conjunction with Asset Owner [OG-ORG-007]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to maintain current inventories of ACME's Technology Assets, Applications and/or Services (TAAS) 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 [IO-ORG-001], in conjunction with Asset Owner [OG-ORG-007], 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, Applications, Services and/or Data (TAASD) that:

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

Procedure / Control Activity: Asset Owner [OG-ORG-007], in conjunction with Systems Administration [IO-WRL-005]:

(1) Maintains an inventory of Technology Assets, Applications, Services and/or Data (TAASD) that includes, but is not limited to: [14]
    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, Application and/or Service (TAAS), per CMMC scoping guidelines:
    a. CUI Asset;
    b. Security Protection Asset (SPA);
    c. Contractor Risk Managed Asset (CRMA)
    d. Specialized Asset (SA); or

[14] *NIST SP 800-171A / CMMC 2.0: 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] | NIST SP 800-171A R3: A.03.04.10.a*