YOUR LOGO GOES HERE

STANDARDIZED OPERATING PROCEDURES (SOP)

ACME Professional Services, LLC

CSOP
Cybersecurity Standardized Operating Procedures

TABLE OF CONTENTS

KEY TERMINOLOGY

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

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

OVERVIEW

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

CUSTOMIZATION GUIDANCE

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

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

VALIDATING NEEDS FOR PROCEDURES / CONTROL ACTIVITIES

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

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

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.

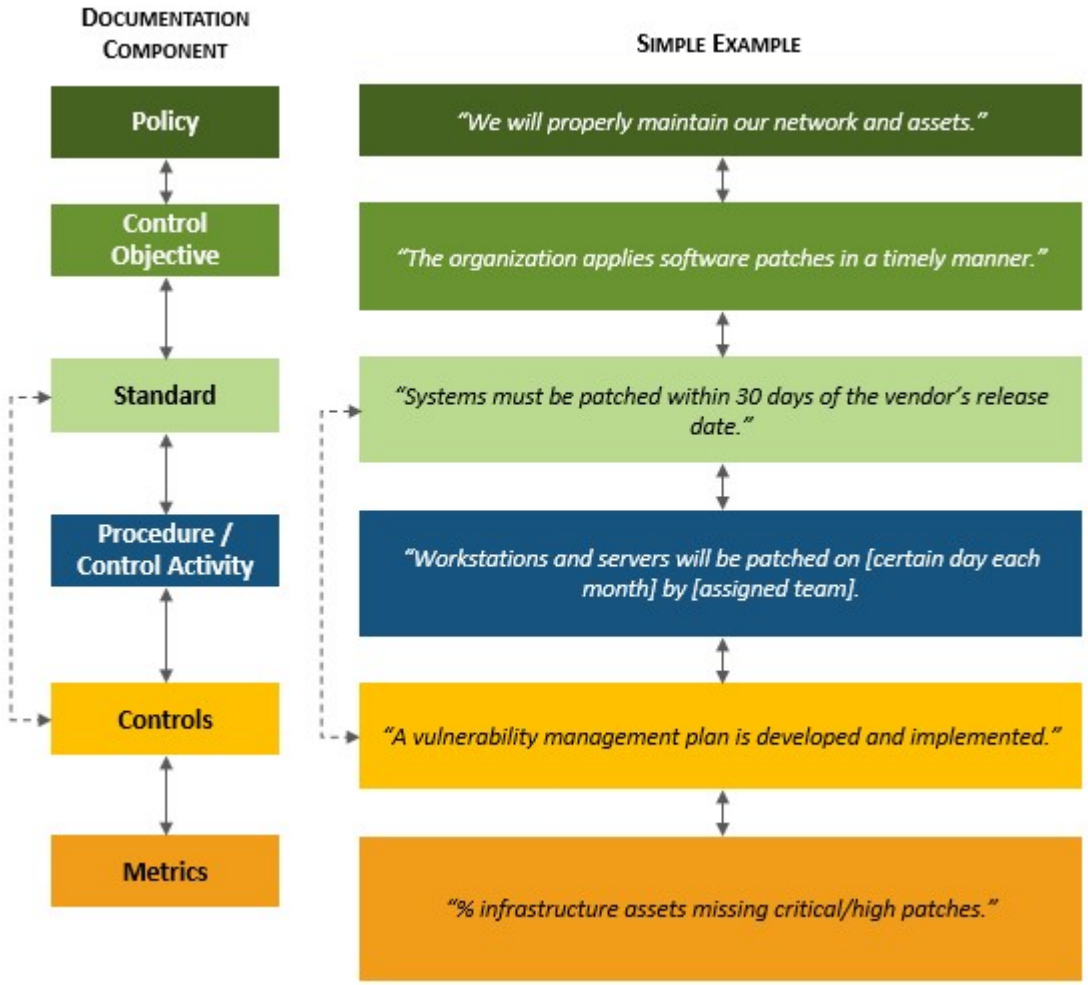
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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.



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;

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.

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

P-GOV-02: PUBLISHING SECURITY & PRIVACY DOCUMENTATION

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

Procedure / Control Activity: Cyber Policy and Strategy Planner [OV-SPP-002], in conjunction with Executive Cyber Leadership [OV-EXL-001], Systems Security Manager [OV-MGT-001] and Cyber Legal Advisor [OV-LGA-001]:

(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 privacy policies and standards in a consolidated document, the Digital Security Program (DSP).
(4) Receives written endorsement from executive management.
(5) Disseminates the DSP to all affected parties to ensure all ACME personnel understand their applicable requirements.
(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.

P-GOV-04: ASSIGNED CYBERSECURITY & PRIVACY RESPONSIBILITIES

Control: Mechanisms exist to assign a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.

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

(1) Leverages the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CSF)[2] for identifying necessary roles and responsibilities:
    a. Establish, document and distribute security policies and procedures;
    b. Monitor and analyze security alerts and information;
    c. Distribute and escalate security alerts to appropriate personnel;
    d. Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
    e. Administer user accounts, including additions, deletions and modifications; and
    f. Monitor and control all access to data.
(2) Utilizes existing HR processes to assign formal roles and responsibilities to employees who have cybersecurity job functions.
(3) Provides written notification to the employee of assigned cybersecurity roles and responsibilities.
(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.

[2] NIST NICE - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

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

P-GOV-05: Measures of Performance

Control: Mechanisms exist to develop, report and monitor cybersecurity and privacy program measures of performance.

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

(1) Based on ACME's aligned cybersecurity and privacy frameworks, develops measures of performance or outcome-based metrics to measure the effectiveness or efficiency of the controls employed across the enterprise.
(2) Communicates awareness and understanding of metrics to stakeholders, including Key Performance Indicators (KPDs) and Key Risk Indicators (KRIs).
(3) Creates and manages a process to share the effectiveness of protection technologies with appropriate stakeholders.
(4) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(5) If necessary, requests corrective action to address identified deficiencies.
(6) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(7) If necessary, documents the results of corrective action and notes findings.
(8) If necessary, requests additional corrective action to address unremediated deficiencies.

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; and
    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; and
        iii. Strategy; and
    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.

Management Intent: The purpose of the Compliance (CPL) procedures / control activities is to ensure safeguards are in place to be aware of and comply with applicable statutory, regulatory and contractual compliance obligations.

P-CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE

Control: Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.

Procedure / Control Activity: Compliance Manager [XX-GRC-005] In conjunction with Governance Manager [XX-GRC-001], Risk Manager [XX-GRC-003], Privacy Officer/Privacy Compliance Manager [OV-LGA-002], Systems Security Manager [OV-MGT-001], Security Architect [SP-ARC-002] and Executive Cyber Leadership [OV-EXL-001]:

(1) Implements appropriate administrative means to document the geographic location of all ACME facilities.
(2) Utilizes the following online resources to identify changes in statutory and/or regulatory data protection requirements that impact all geographical locations:
    a. **US States** - http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx
    b. **US Federal** - https://content.next.westlaw.com/Browse/Home/PracticalLaw
    c. **International** - https://www.dlapiperdataprotection.com
(3) Consults with stakeholders in Legal to determine if there are any new contractual obligation changes.
(4) Documents any changes to statutory, regulatory and contractual compliance obligations.
(5) Assembles key stakeholders to perform a review of ACME's policies and standards to address necessary changes, if necessary.
(6) Incorporates feedback into an updated version of ACME's policies and standards.
(7) By the end of the [1st, 2nd, 3rd, 4th] quarter of the calendar year, oversees the change management process to release the changes from draft to production.
(8) 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.
(9) If necessary, requests corrective action to address identified deficiencies.
(10) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(11) If necessary, documents the results of corrective action and notes findings.
(12) If necessary, requests additional corrective action to address unremediated deficiencies.

P-CPL-02: SECURITY & PRIVACY CONTROLS OVERSIGHT

Control: Mechanisms exist to provide a security & privacy controls oversight function that reports to the organization's executive leadership.

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) Develops a continuous monitoring strategy that includes effectiveness, compliance and change monitoring: [10]
    a. Establishing the system-level metrics to be monitored;
    b. Establishing organization-defined frequencies for monitoring and for assessing control effectiveness;
    c. Ongoing control assessments in accordance with the continuous monitoring strategy;
    d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
    e. Correlation and analysis of information generated by control assessments and monitoring;
    f. Response actions to address results of the analysis of control assessment and monitoring information; and
    g. Reporting the cybersecurity and privacy status of the system to organization-defined personnel or roles per organization-defined frequency.
(2) Implements appropriate administrative means to ensure controls are sufficient for capturing, protecting and reviewing logs from all system components in accordance with ACME requirements to centrally manage and identify anomalies or suspicious activity to ensure the continued effectiveness of cybersecurity and privacy controls. This includes:

[10] *NIST SP 800-171A / CMMC assessment criteria 3.12.3 / CA.L2-3.12.3[a]*

Management Intent: The purpose of the Configuration Management (CFG) procedures / control activities is to establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced.

P-CFG-01: CONFIGURATION MANAGEMENT PROGRAM

Control: Mechanisms exist to facilitate the implementation of configuration management controls.

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) Develops an organization-wide configuration management program.
(2) Documents a configuration management policy and standards in a single document, the Cybersecurity & Data Protection Program (CDPP). [11]
(3) Requires data/process owners and asset custodians to:
    a. Document function-specific procedures in a Cybersecurity Standardized Operating Procedures (CSOP), or similar format;
    b. Identify applicable statutory, regulatory and contractual obligations (see CDPP Applicability Matrix); and
    c. Include the identification and assignment of roles and responsibilities among internal and external stakeholders.
(4) Implements appropriate administrative and technical means to ensure controls are sufficient for organization-wide configuration management governance that includes:
    a. As systems continue through the System Development Life Cycle (SDLC), new configuration items are identified and as existing configuration items may no longer need and are retired; and
    b. Configuration management plans satisfy the requirements of ACME's configuration management policy while being tailored to individual systems through approved deviations processes, as necessary.
(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-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS

Control: Mechanisms exist to develop, document and maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards.

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

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure baseline system hardening configuration for all ACME-owned or managed assets comply with applicable legal, statutory and regulatory compliance obligations throughout the System Development Life Cycle (SDLC). 12
(2) Includes hardware, software, firmware and documentation in baseline configurations. Where technically feasible, technology platforms align with industry-recommended hardening recommendations, including but not limited to: 13
    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:

[11] *NIST SP 800-171A / CMMC assessment criteria 3.4.8[a] / CM.L2-3.4.8[a]*
[12] *NIST SP 800-171A / CMMC assessment criteria 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]*
[13] *NIST SP 800-171A / CMMC assessment criteria 3.4.1[b] / CM.L2-3.4.1[b]*