YOUR LOGO GOES HERE

CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

NIST CYBERSECURITY FRAMEWORK 2.0

ACME Consulting Partners, 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 90% of the content as part of the template that would leave the remaining 10% 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.

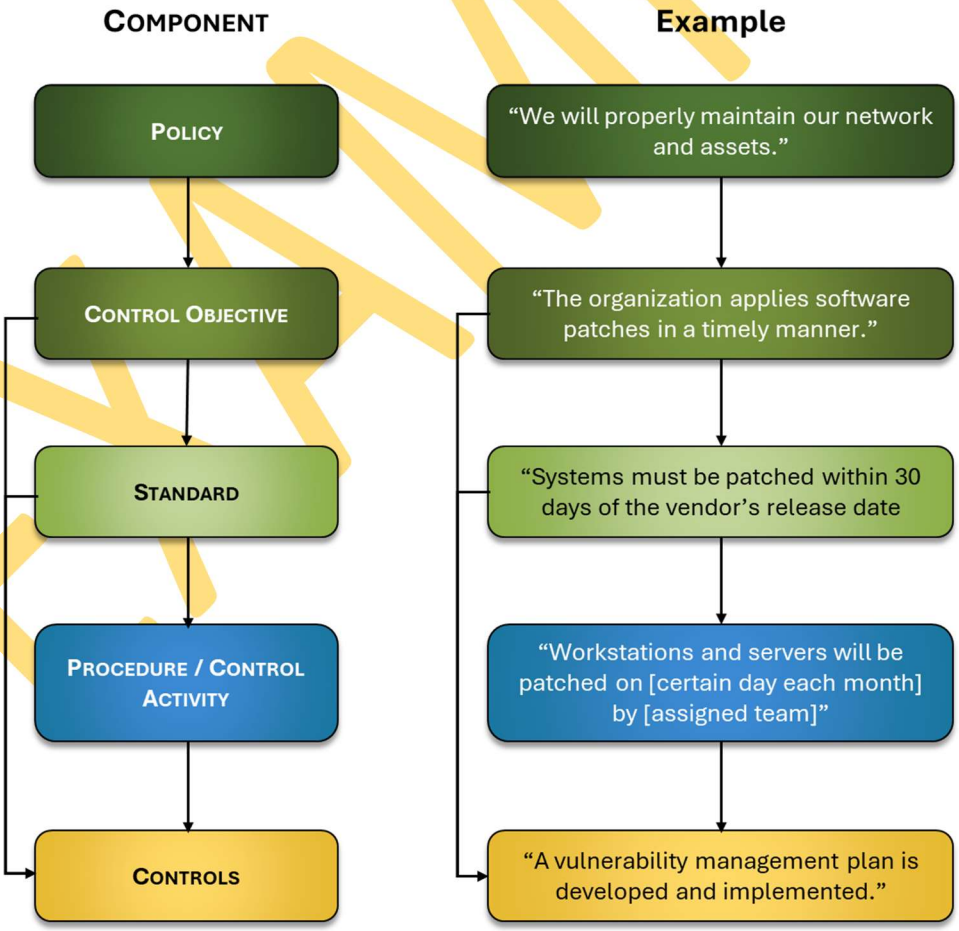
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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 & data 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 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 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*

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]:

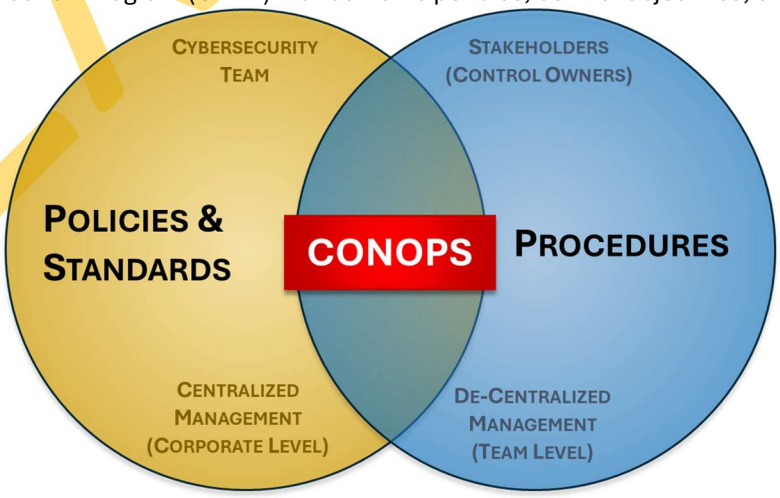
(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure baseline system hardening configurations for all ACME-owned or managed assets comply with applicable legal, statutory and regulatory compliance obligations throughout the System Development Life Cycle (SDLC).
(2) 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:
    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) Technology platforms that include, but are not limited to:
    a. Server-Class Systems
        i. Microsoft Server 2003
        ii. Microsoft Server 2008
        iii. Microsoft Server 2012
        iv. Microsoft Server 2016
        v. Microsoft Server 2018
        vi. Microsoft Server 2020
        vii. Microsoft Server 2022
        viii. Red Hat Enterprise Linux (RHEL)
        ix. Unix
        x. Solaris
    b. Workstation-Class Systems
        i. Microsoft XP
        ii. Microsoft 7
        iii. Microsoft 8
        iv. Microsoft 10
        v. Microsoft 11
        vi. Apple
        vii. Fedora (Linux)
        viii. Ubuntu (Linux)
        ix. 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
        ii. Windows SQL Server
        iii. Windows SQL Express
        iv. Oracle
        v. DB2
(4) Ensures that system hardening includes, but is not limited to:

a. 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.
b. Configuring and documenting only the necessary ports, protocols and services to meet business needs;
c. 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;
d. 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
e. 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).

(5) Documents and validates security parameters are configured to prevent misuse.
(6) Authorizes deviations from standard baseline configurations in accordance with ACME's change management processes, prior to deployment, provisioning or use.
(7) 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.
(8) 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.
(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.

Supporting Policies & Standards

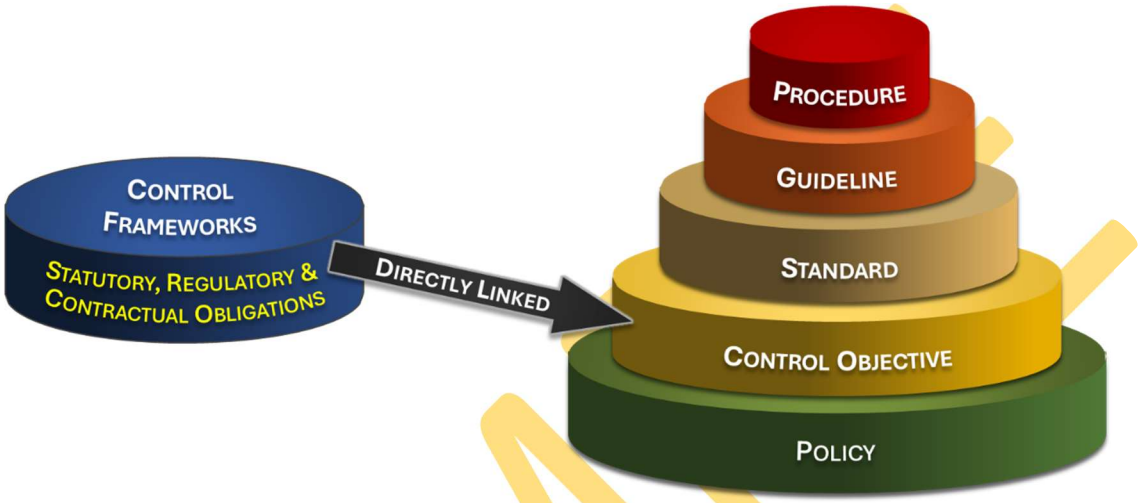
While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with Cybersecurity And Data Protection Program (CDPP) that contains policies, control objectives, standards and guidelines.



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 & data protection program.

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

Control: Mechanisms exist to facilitate the implementation of cybersecurity & 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 & data privacy governance program to provide complete coverage for all cybersecurity & data privacy-related controls needed to address statutory, regulatory and contractual obligations, as well as to address possible threats to data and or assets.
(2) Documents the ACME cybersecurity & data privacy governance program in a single document, the Cybersecurity And 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-01.1: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | STEERING COMMITTEE & PROGRAM OVERSIGHT

Control: Mechanisms exist to coordinate cybersecurity, data privacy and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.

Procedure / Control Activity: Executive Cybersecurity Leadership [OG-WRL-007]:

(1) Develops a steering committee to coordinate cybersecurity, data privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, data privacy and business executives.
(2) Defines the composition of the steering committee (e.g., identifies key cybersecurity, data privacy and business executives).
(3) Assigns roles to steering committee personnel:
    a. Chair;
    b. Vice Chair; and
    c. Committee Staff;
(4) Defines the expected conduct the steering committee meetings to ensure cybersecurity & data privacy solutions and services follows the CARES principles:
    a. Competitive in scope and price over the long term;
    b. Adaptable and customized to meet stakeholder needs;
    c. Resolute in delivering timely solutions that address present and emerging risks;
    d. Equitable in allocating costs and services between various stakeholders in a fair and consistent manner; and
    e. Stable in supporting cost-effective, fiscally-prudent operations and in building long-term relationships with stakeholders and program/service partners.
(5) Requires steering committee members to attend each steering committee meeting or send a representative.
(6) Requires the steering committee to keeps and prepare meeting minutes for review and approval.
(7) Requires the steering committee to meet at least quarterly (in-person or teleconference).
(8) Requires a quorum of committee members to hold a meeting;
(9) Governs the review of cybersecurity & data privacy-related projects/initiatives accordingly:
    a. Each project must be assigned a sponsor, typically from the submitting department;

b. Projects must be presented in writing to the Committee Chair and will contain a business case of adequate detail to allow the steering committee to assess and prioritize the work and shall include cost and personnel resource estimates as well as funding sources;
c. The Committee Chair must review the submission for completeness and accuracy prior to setting the submission on an agenda;
d. Submissions must be distributed electronically to members of the steering committee prior to the agenda date;
e. The project sponsor may be asked to make a presentation to the steering committee on the project at the steering committee meeting; and
f. The steering committee must review and discuss the submission and accept a motion from the steering committee to take one of the following actions:
    i. Approve the project;
    ii. Return the project to the department for revision or further information;
    iii. Table the project for later action;
    iv. Deny the project; or
    v. Other action as suggested in the motion.

(10) A simple majority vote of the committee members present is required for an affirmative vote. In the event of a tie vote, at the discretion of the Committee Chair, one of the following options may be used:
a. Resolve the impasse by further discussion and calling for an additional vote; or
b. Send the submission back for further analysis, clarification or revision.

(11) 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.

(12) If necessary, requests corrective action to address identified deficiencies.
(13) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(14) If necessary, documents the results of corrective action and notes findings.
(15) If necessary, requests additional corrective action to address unremediated deficiencies.

P-GOV-01.2: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | STATUS REPORTING TO GOVERNING BODY

Control: Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.

Procedure / Control Activity: Executive Cybersecurity Leadership [OG-WRL-007]:

(1) Develops a steering committee to coordinate cybersecurity, data privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, data privacy and business executives.
(2) Defines the composition of the steering committee (e.g., identifies key cybersecurity, data privacy and business executives).
(3) Assigns roles to steering committee personnel:
a. Chair;
b. Vice Chair; and
c. Committee Staff;
(4) Defines the expected conduct the steering committee meetings to ensure cybersecurity & data privacy solutions and services follows the CARES principles:
a. Competitive in scope and price over the long term;
b. Adaptable and customized to meet stakeholder needs;
c. Resolute in delivering timely solutions that address present and emerging risks;
d. Equitable in allocating costs and services between various stakeholders in a fair and consistent manner; and
e. Stable in supporting cost-effective, fiscally-prudent operations and in building long-term relationships with stakeholders and program/service partners.
(5) Requires steering committee members to attend each steering committee meeting or send a representative.
(6) Requires the steering committee to keeps and prepare meeting minutes for review and approval.
(7) Requires the steering committee to meet at least quarterly (in-person or teleconference).
(8) Requires a quorum of committee members to hold a meeting;
(9) Governs the review of cybersecurity & data privacy-related projects/initiatives accordingly:
a. Each project must be assigned a sponsor, typically from the submitting department;

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 [OG-ORG-005] In conjunction with Governance Manager [OG-ORG-001], Risk Manager [OG-ORG-003], Privacy Compliance [OG-WRL-008], Systems Security Management [OG-WRL-014], Cybersecurity Architecture [DD-WRL-001] and Executive Cybersecurity Leadership [OG-WRL-007]:

(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-01.2: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE | COMPLIANCE SCOPE

Control: Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.

Procedure / Control Activity: Compliance Manager [OG-ORG-005] In conjunction with Governance Manager [OG-ORG-001], Risk Manager [OG-ORG-003], Privacy Compliance [OG-WRL-008], Systems Security Management [OG-WRL-014], Cybersecurity Architecture [DD-WRL-001] and Executive Cybersecurity Leadership [OG-WRL-007]:

(1) Implements appropriate administrative means to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations by:
    a. Conducting an annual review of applicable statutory, regulatory and/or contractual compliance obligations;
    b. Determining the Minimum Compliance Controls (MCR) necessary to address compliance obligations;
    c. Determining the systems, applications, services and third-parties that are applicable to the identified controls;
    d. Documenting the scope of statutory, regulatory and/or contractual compliance obligations;
    e. Identifying the stakeholders who are responsible for "control ownership"; and
    f. Sharing updated compliance scoping documentation with affected stakeholders so that all parties involved are in agreement on the scope of compliance efforts.
(2) 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-CPL-02: Cybersecurity & Data Protection Controls Oversight

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

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 a continuous monitoring strategy that includes effectiveness, compliance and change monitoring: [30]
    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 & data 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 & data privacy controls. This includes:
    a. Reviewing the following, at least daily:
        i. All security events;
        ii. Logs of all system components that store, process or transmit sensitive/regulated data or that could impact the security of sensitive/regulated data;
        iii. Logs of all critical system components; and
        iv. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
            1. Firewalls;
            2. Intrusion Detection Systems (IDS);
            3. Intrusion Prevention Systems (IPS);
            4. Authentication servers (e.g., Active Directory domain controllers); and
            5. E-commerce redirection servers.
    b. Reviewing logs of all other system components periodically based on ACME's policies and risk management strategy, as determined by ACME's annual risk assessment; and
    c. Following up exceptions and anomalies identified during the review process.
(3) Develops processes for the timely detection and reporting of failures of security controls on critical systems or systems containing sensitive/regulated data, including but not limited to failure of:
    a. Firewalls;
    b. IDS/IPS;
    c. FIM;
    d. Antimalware;
    e. Physical access controls;
    f. Logical access controls;
    g. Audit logging mechanisms; and
    h. Segmentation controls (if used); and
(4) Develops processes to respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls include:

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