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.

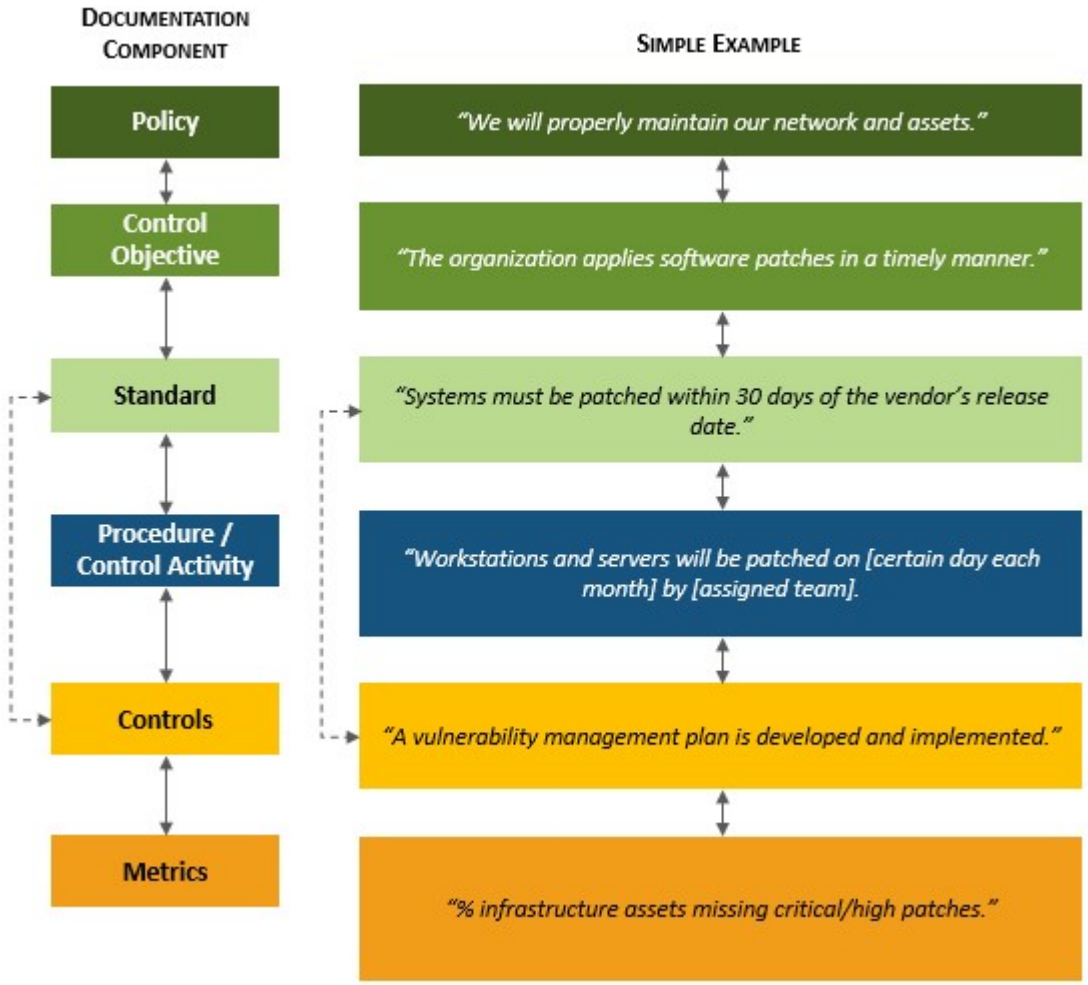
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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-01: DIGITAL SECURITY GOVERNANCE PROGRAM

Control: Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance 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 digital security governance program to provide complete coverage for all cybersecurity and 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 digital security governance program in a single document, the Digital Security Program (DSP).
(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: DIGITAL SECURITY GOVERNANCE PROGRAM | STEERING COMMITTEE

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

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001]:

(1) Develops a steering committee to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives.
(2) Defines the composition of the steering committee (e.g., identifies key cybersecurity, 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 and privacy solutions and services follows the CARES principles:
    a. **C**ompetitive in scope and price over the long term;
    b. **A**daptable and customized to meet stakeholder needs;
    c. **R**esolute in delivering timely solutions that address present and emerging risks;
    d. **E**quitable in allocating costs and services between various stakeholders in a fair and consistent manner; and
    e. **S**table 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 and 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: DIGITAL SECURITY 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 and privacy program.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001]:

(1) Develops a steering committee to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives.
(2) Defines the composition of the steering committee (e.g., identifies key cybersecurity, 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 and privacy solutions and services follows the CARES principles:
    a. **C**ompetitive in scope and price over the long term;
    b. **A**daptable and customized to meet stakeholder needs;
    c. **R**esolute in delivering timely solutions that address present and emerging risks;
    d. **E**quitable in allocating costs and services between various stakeholders in a fair and consistent manner; and
    e. **S**table 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 and 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

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; [8]
        ii. Reviewed; [9]
        iii. Approved or Disapproved; [10] and
        iv. Documented. [11]
(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.

[8] *NIST SP 800-171A / CMMC assessment criteria 3.4.3[a] / CM.L2-3.4.3[a]*
[9] *NIST SP 800-171A / CMMC assessment criteria 3.4.3[b] / CM.L2-3.4.3[b]*
[10] *NIST SP 800-171A / CMMC assessment criteria 3.4.3[c] / CM.L2-3.4.3[c]*
[11] *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.

Management Intent: The purpose of the Third-Party Management (TPM) procedures / control activities is to ensure that risk associated with third-parties are minimized or avoided.

P-TPM-01: THIRD-PARTY MANAGEMENT

Control: Mechanisms exist to facilitate the implementation of third-party management controls.

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

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for managing third-party service providers' compliance with cybersecurity, privacy and service delivery requirements included in third-party contracts by:
    a. Requiring data/process owners maintain and implement procedures to manage service providers that includes:
        i. Maintaining a list of service providers;
        ii. Maintaining a written agreement that includes an acknowledgment that the service providers are responsible for the security of sensitive/regulated data the service providers possess or otherwise store, process or transmit on behalf of ACME, or to the extent that they could impact the security of ACME;
        iii. Monitoring and ensuring there is an established process for engaging service providers, including proper due diligence prior to engagement;
        iv. Maintaining a program to monitor service providers' compliance status at least annually; and
        v. Maintaining information about which requirements are managed by each service provider, and which are managed by ACME.
    b. Utilizing the process of due diligence:
        i. Direct observations;
        ii. Reviews of policies and procedures; and
        iii. Reviews of supporting documentation.
(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-TPM-01.1: THIRD-PARTY MANAGEMENT | THIRD-PARTY INVENTORIES

Control: Mechanisms exist to maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.

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

(1) Uses Implements appropriate administrative and technical means to maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of ACME' technology assets and data.
(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.