Your Logo
Will Be
Placed Here

STANDARDIZED OPERATING PROCEDURES (SOP)

ACME Business Consulting, LLC

ISO 27002

WISP
Written Information Security Program

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

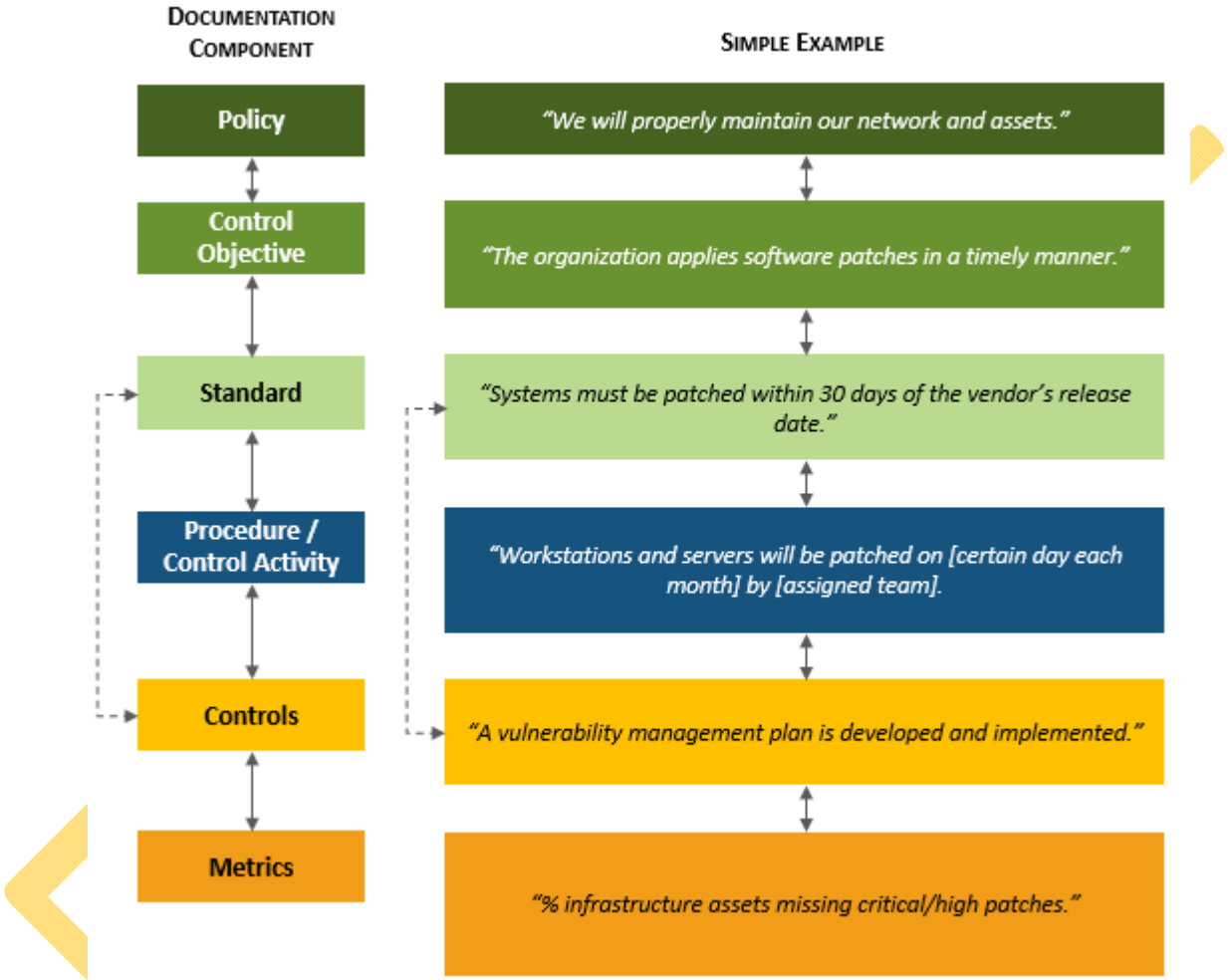
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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!

[1] NIST NICE Cybersecurity Workforce Framework - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

NIST NICE Cybersecurity Workforce Framework – Work Categories

EXAMPLE PROCEDURE

This example is a configuration procedure from section **10.1.1.1 (Secure 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

Control Objective: The organization develops and controls configuration standards for all system components that are consistent with industry-accepted system hardening standards. [2] *[the control objective is meant to address the statutory, regulatory and contractual requirements identified in the footnote (see bottom of page in the footer section)]*

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.

[2] NIST 800-53 rev4 CM-2 & CM-6 | FedRAMP | NIST 800-171 3.4.1 & 3.4.2 | PCI DSS 1.1 & 1.1.1 | NIST CSF PR.IP-1 | DFARS 252.204-7008 | CSC 3.1 | CCM GRM-01 & IVS-07 | COBIT5 BAI10.02 | NISPOM 8-202, 8-311 & 8-610

(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).

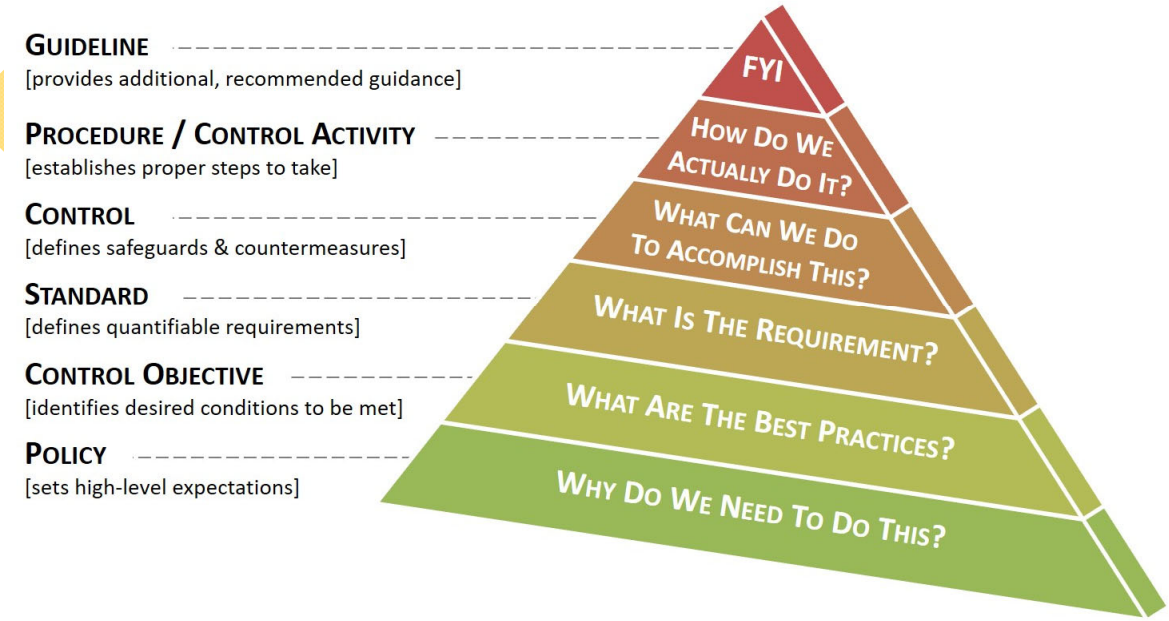
(4) Documents and validates security parameters are configured to prevent misuse.
(5) Authorizes deviations from standard baseline configurations in accordance with ACME's change management processes, prior to deployment, provisioning, or use.
(6) Validates and refreshes configurations on a regular basis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

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 ComplianceForge's ISO 27002-based Written Information Security Program (WISP) that contains policies, control objectives, standards and guidelines.

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

(1) Core policy that establishes management's intent;
(2) Control objective that identifies leading practices;
(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.



Cybersecurity Documentation Hierarchy

2.1.4 *Special Interest Groups*

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.[21]

2.1.4.1 *Contacts With Security Groups & Associations*

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- 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?
- 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?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: The organization establishes and institutionalizes contact with selected groups and associations within the security community to: [22]

- Facilitate ongoing security education and training for organizational personnel;
- Maintain currency with recommended security practices, techniques and technologies; and
- Share current security-related information including threats, vulnerabilities and incidents.

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) Researches, establishes and maintains formal contact with select groups and / or associations within the cybersecurity and communities. Security groups and associations include, but are not limited to:
    a. Special Interest Groups (SIGs);
    b. Professional associations; and
    c. Peer groups of cybersecurity and privacy professionals in similar organizations.
(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.

2.1.4.2 *Security Industry Alerts & Notification Process*

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- 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?
- 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?

[21] ISO/IEC 27002:2013 – 6.1.4

[22] HIPAA 164.308(A)(5)(ii) & (ii)(A) | PCI DSS v3.2 5.1.2 & 6.1 | NIST CSF v1.1 ID.RA-2 & RS.CO-5 | NY DFS 500.10

2.2.1.1 Access Control For Mobile Devices

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- 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?
- 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?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: The organization: [29]

- Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;
- Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;
- Monitors for unauthorized connections of mobile devices to organizational information systems;
- Enforces requirements for the connection of mobile devices to organizational information systems;
- Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
- Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk; and
- Applies inspection measures to mobile devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.

Procedure / Control Activity: Systems Security Developer [SP-SYS-001], in conjunction with Identity & Access Specialist [XX-IAC-001] and Systems Security Manager [OV-MGT-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to implement access control for mobile devices, in accordance with ACME policies and standards:
   a. Loss / Theft. Immediately notify ACME management if a mobile device is lost or stolen and the user must alert management to the circumstance of the loss and the data contained on the mobile device;
   b. Conduct: Users must conduct themselves in accordance with ACME's Acceptable Use parameters (*Annex5: Rules of Behavior (Acceptable & Unacceptable Use)*);
   c. Passwords: A password or PIN with a minimum of four (4) characters must be used to log onto the device
   d. Lockout. The mobile device must be set to delete all data or lock internally after ten (10) unsuccessful attempts to enter a password or PIN.
   e. Encryption: The data on the mobile device must be encrypted.
   f. Message Storage Limits. Users may not store more than two hundred (200) messages or fourteen (14) days of messages on a mobile device.
   g. Data Backups: If the user backs up the data from the mobile device to another device that is not encrypted (e.g., backing up a tablet using an unencrypted computer) then the backup data must be encrypted.
   h. Software Protections: Applications that create, store, access, send or receive ePHI must meet ACME security standards and custom developed applications used on mobile devices must undergo a security design review.
   i. Antimalware: Antimalware software must be installed on mobile devices that are capable of running such software:
      i. Android: Android devices are required to have antimalware software installed.
      ii. Windows: Windows devices are required to have antimalware software installed.
      iii. Apple: The Apple iOS is not currently capable of running antimalware software, since no such software exists, based on the design of the iOS.
   j. Updates: Mobile device and installed applications must be kept updated with the latest vendor software releases:
      i. Operating Systems: The most recent operating system available for the mobile data device must be used.

[29] ISO/IEC 27002:2013 – 6.2.1 | NIST CSF v1.1 PR.AC-3

ii. Applications: Available security updates for any applications must be applied in a regular and timely manner unless instructed otherwise by ACME IT staff.

k. Rooting: Users must not circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., "jailbreaking") and users must not tamper with the mobile device by using unauthorized software, hardware, or other methods.

l. Wireless: Users are required to utilize good judgment when connecting the mobile device to other devices and networks:

i. Bluetooth: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.

ii. WiFi: Users may use only secure (e.g., WPA2) WiFi networks known to be trustworthy.

iii. Cellular: ACME is not responsible for overages or data plans for cellular usage.

(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.

2.2.1.2 CENTRAL MANAGEMENT OF MOBILE DEVICES

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure's tasks
- 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?
- 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?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: The organization centrally manages mobile devices.

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) Uses vendor-recommended settings and industry-recognized secure practices to ensure are sufficient for managing mobile devices by:

a. Centrally-managing a mobile device management solution;

b. Managing passwords in accordance with ACME's existing password standards;

c. Maintaining an inventory of all authorized mobile devices used to store and access ACME data;

d. Defining approved application stores for mobile devices accessing or storing sensitive data; and

e. Alerting security personnel when mobile devices are rooted or jailbroken.

(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.