YOUR LOGO GOES HERE

CORE FUNDAMENTALS PROCEDURES

SECURE CONTROLS FRAMEWORK

CORE FUNDAMENTALS

ACME Business Operations, LLP

Table of Contents

OVERVIEW, INSTRUCTIONS & EXAMPLE

The Secure Controls Framework (SCF) created the Cybersecurity Oversight, Resilience and Enablement (CORE) initiative to help organizations tailor cybersecurity and data protection controls to fit its specific needs. The CORE Fundamentals is a tailored set of sixty-eight (68) controls that are specifically designed for Small and Medium Businesses (SMB) to protect People, Processes, Technologies, Data and Facilities (PPTDF) against common threats.

The **CORE Fundamentals Procedures** document provides a catalog of procedures templates that correspond to ACME Business Operations, LLP (ACME) policies and standards. The expectation is for control owners/operators to tailor these procedures templates for the specific use case.

KEY TERMINOLOGY

With the CORE Fundamentals Procedures document, 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 CORE Fundamentals Procedures document, 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).

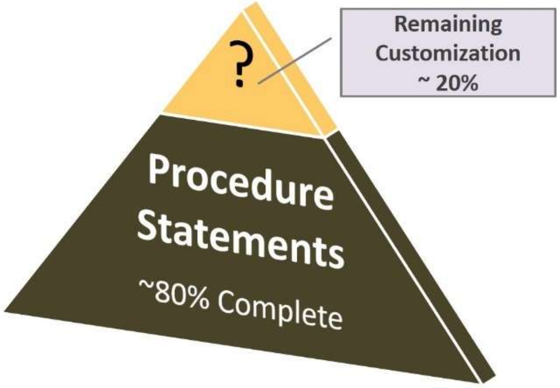
OVERVIEW

The CORE Fundamentals Procedures document is a catalog of procedure/control activity statements. These are templates that require modification to suit the specific needs of the organization.

CUSTOMIZATION GUIDANCE

The content of the CORE Fundamentals Procedures document 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 CORE Fundamentals Procedures document 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.

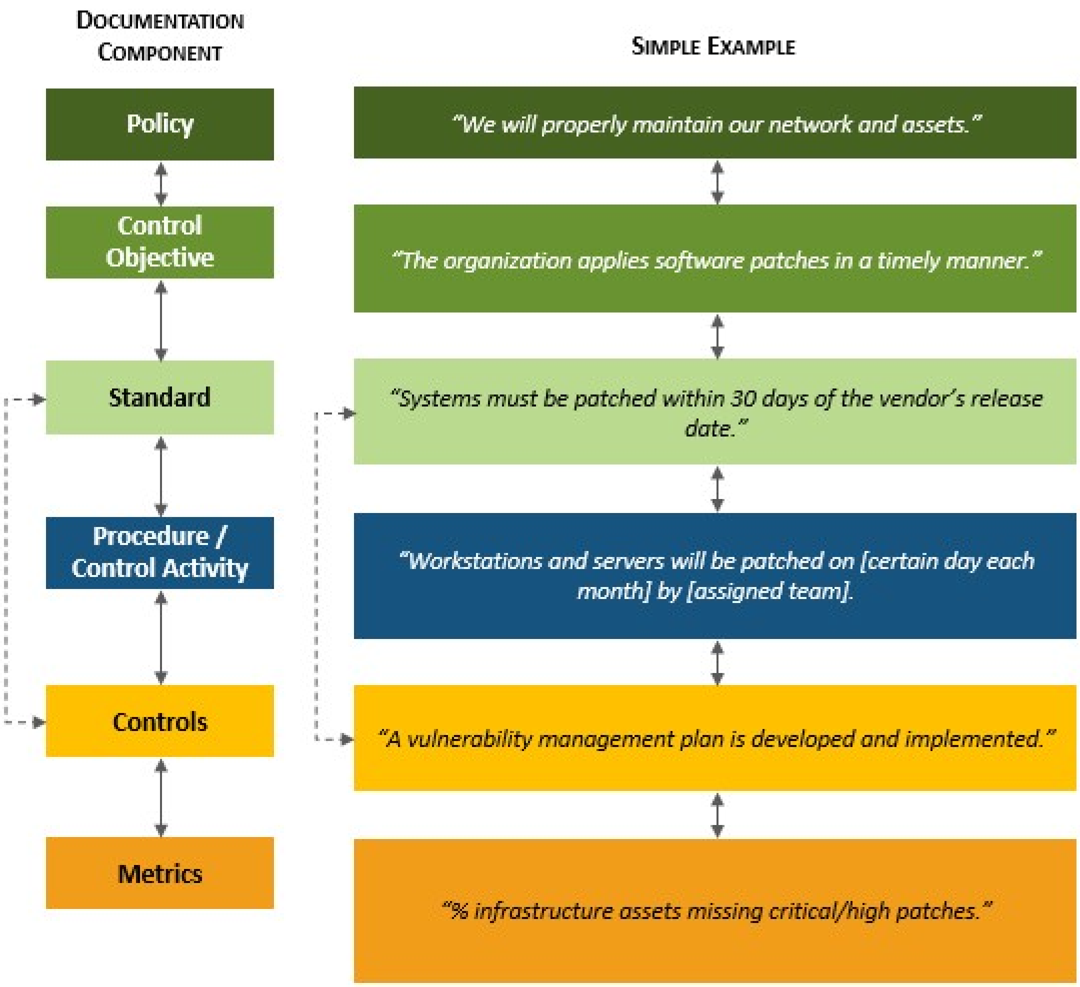
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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.

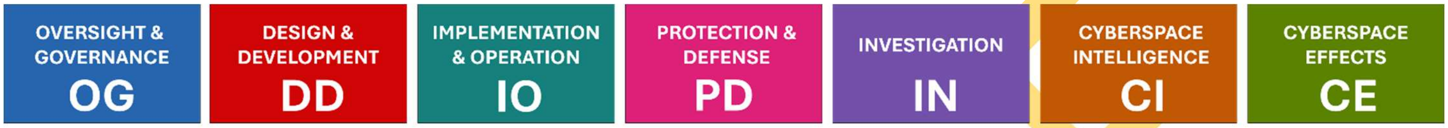


Documentation Component	Simple Example
Policy	*"We will properly maintain our network and assets."*
Control Objective	*"The organization applies software patches in a timely manner."*
Standard	*"Systems must be patched within 30 days of the vendor's release date."*
Procedure / Control Activity	*"Workstations and servers will be patched on [certain day each month] by [assigned team].*
Controls	*"A vulnerability management plan is developed and implemented."*
Metrics	*"% infrastructure assets missing critical/high patches."*

NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

The CORE Fundamentals Procedures document 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 CORE Fundamentals Procedures document 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

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

▪ Databases

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.

CHANGE MANAGEMENT (CHG) PROCEDURES

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 [IO-ORG-002], in conjunction with Systems Security Management [OG-WRL-014] and Executive Cybersecurity Leadership [OG-WRL-007]:

(1) Develops, implements and governs controls that are sufficient for managing and documenting change management activities that includes:[17]
  - a. A formal, documented change management program; and
  - b. Processes to facilitate the implementation of changes.

(2) Required changes to be:
  - a. Reviewed by an individual with the appropriate authority and knowledge to understand the impact of the change; [18]
  - b. Approved by a ACME employee with the appropriate authority and knowledge to understand the impact of the change; and
  - c. Approved by ACME's Change Control Board (CCB);

(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-CHG-02: CONFIGURATION CHANGE CONTROL

Control: Mechanisms exist to govern the technical configuration Change Control processes.

Procedure / Control Activity: Change Control Manager [IO-ORG-002], in conjunction with Systems Security Management [OG-WRL-014] and Executive Cybersecurity Leadership [OG-WRL-007]:

(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; [19]
    - ii. Reviewed; [20]
    - iii. Approved or Disapproved; [21]and
    - iv. Documented. [22]

[17] *NIST SP 800-171A R3: A.03.04.03.d[01]*

[18] *NIST SP 800-171A R3: A.03.04.03.d[02]*

[19] *NIST SP 800-171A / CMMC 2.0: 3.4.3[a] / CM.L2-3.4.3[a]*

[20] *NIST SP 800-171A / CMMC 2.0: 3.4.3[b] / CM.L2-3.4.3[b]*

[21] *NIST SP 800-171A / CMMC 2.0: 3.4.3[c] / CM.L2-3.4.3[c]*

[22] *NIST SP 800-171A / CMMC 2.0: 3.4.3[d] / CM.L2-3.4.3[d]*

(2) Provides proactive governance for technology-related changes that includes, but is not limited to:[23]
   a. Preventative maintenance of production systems, applications and/or services;
   b. Reactive / emergency maintenance of production systems, applications and/or services;
   c. Changes to baseline configurations for production technology platforms used by ACME that includes:
      i. Server-class systems;
      ii. Workstation-class systems;
      iii. Network devices;
      iv. Mobile devices;
      v. Databases;
      vi. Major applications;
      vii. Minor applications;
      viii. Cloud-based services; and
      ix. Embedded technologies.

(3) Oversees the implementation of approved configuration-controlled changes to affected systems, applications and/or services.[24]

(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-CHG-03: Security Impact Analysis for Changes

Control: Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.

Procedure / Control Activity: Systems Administration [IO-WRL-005], in conjunction with Asset Owner [OG-ORG-007] and Change Control Manager [IO-ORG-002]:

(1) Follows published ACME Change Control processes to evaluate the security impact for changes that includes prior to the implementation of a change, ACME's cybersecurity personnel must: [25]
   a. Review the cybersecurity-related implications of the change; and
   b. Provide expert-level guidance on risk remediation actions for identified cybersecurity issues; and

(2) Where technically feasible, from a test environment, tests proposed changes specifically to assess the security functions of the system(s) to verify that those functions are:
   a. Implemented correctly;
   b. Operate as intended; and
   c. Meet the security requirements for the system.

(3) Performs a security impact analysis to understand security control requirements and review system design documentation to understand control implementation and how specific changes might affect the controls. The analysis process includes a review of: [26]
   a. Separate development/test and production environments;
   b. Separation of duties between development/test and production environments;
   c. Production data (live data) are not used for testing or development; and
   d. Removal of test data and accounts before production systems become active.

(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

[23] *NIST SP 800-171A R3: A.03.04.03.a*
[24] *NIST SP 800-171A R3: A.03.04.03.c[01]*
[25] *NIST SP 800-171A R3: A.03.04.03.b[01]*
[26] *NIST SP 800-171A / CMMC 2.0: 3.4.4 / CM.L2-3.4.4[a] | NIST SP 800-171A R3: A.03.04.04.a*