Your Logo
Will Be
Placed Here

STANDARDIZED OPERATING PROCEDURES (SOP)

ACME Business Consulting, LLC

NIST
Cybersecurity Framework
CSOP
Cybersecurity Standardized Operating Procedures

Table of Contents

Overview, Instructions & Example 5
Key Terminology 5
Overview 5
Customization Guidance *5*
Validating Needs for Procedures / Control Activities *5*
Procedures Documentation 5
NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework *6*
Example *7*
Supporting Policies & Standards *10*

Known Compliance Requirements 11
Statutory Requirements *11*
Regulatory Requirements *11*
Contractual Requirements *11*

Cybersecurity Governance (GOV) 12
P-GOV-01: Publishing Security & Privacy Policies 12
P-GOV-02: Assigned Security Responsibilities 12
P-GOV-03: Measures of Performance 13

Asset Management (AST) 15
P-AST-01: Asset Inventories 15
P-AST-02: Network Diagrams & Data Flow Diagrams (DFDs) 17
P-AST-03: Removal of Assets 17

Business Continuity & Disaster Recovery (BCD) 19
P-BCD-01: Contingency Plan 19
P-BCD-02: Contingency Plan Root Cause Analysis (RCA) & Lessons Learned 19
P-BCD-03: Contingency Plan Update 20
P-BCD-04: Data Backups 21
P-BCD-05: Information System Recovery & Reconstitution 22

Capacity & Performance Planning (CAP) 23
P-CAP-01: Capacity & Performance Management 23

Change Management (CHG) 24
P-CHG-01: Configuration Change Control 24

Compliance (CPL) 26
P-CPL-01: Statutory, Regulatory & Contractual Compliance 26
P-CPL-02: Security Controls Oversight 27

Configuration Management (CFG) 28
P-CFG-01: System Hardening Through Baseline Configurations 28
P-CFG-02: Least Functionality 30

Continuous Monitoring (MON) 32
P-MON-01: Continuous Monitoring 32
P-MON-02: Monitoring Reporting 33
P-MON-03: Anomalous Behavior 34
P-MON-04: Insider Threats 34
P-MON-05: Third-Party Threats 35
P-MON-06: Unauthorized Activities 37

Cryptographic Protections (CRY) 38
P-CRY-01: Transmission Confidentiality 38
P-CRY-02: Transmission Integrity 39
P-CRY-03: Encrypting Data At Rest 39

Data Classification & Handling (DCH) 41
P-DCH-01: Data & Asset Classification 41
P-DCH-02: Physical Medial Disposal 42

P-DCH-03: Removable Media Security 43

Endpoint Security (END) 44
P-END-01: Malicious Code Protection (Anti-Malware) 44
P-END-02: File Integrity Monitoring (FIM) 45
P-END-03: Mobile Code 46

Human Resources Security (HRS) 48
P-HRS-01: Human Resources Security Management 48

Identification & Authentication (IAC) 49
P-IAC-01: User Provisioning & De-Provisioning 49
P-IAC-02: Account Management 50
P-IAC-03: Least Privilege 51

Incident Response (IRO) 53
P-IRO-01: Incidents Response Operations 53
P-IRO-02: Incident Handling 53
P-IRO-03: Indicators of Compromise (IOC) 54
P-IRO-04: Incident Response Plan (IRP) 55
P-IRO-05: IRP Update 56
P-IRO-06: Coordination with Related Plans 57
P-IRO-07: Integrated Security Incident Response Team (ISIRT) 58
P-IRO-08: Chain of Custody & Forensics 58
P-IRO-09: Incident Monitoring & Tracking 59
P-IRO-10: Incident Reporting 60
P-IRO-11: Root Cause Analysis (RCA) & Lessons Learned 61

Maintenance (MNT) 62
P-MNT-01: Controlled Maintenance 62
P-MNT-02: Non-Local Maintenance 63

Network Security (NET) 65
P-NET-01: Network Security Management 65
P-NET-02: Layered Defenses 65
P-NET-03: Remote Access 67

Physical & Environmental Security (PES) 68
P-PES-01: Physical Access Control 68
P-PES-02: Monitoring Physical Access 69
P-PES-03: Information Leakage Due To Electromagnetic Signals Emanations 70

Project & Resource Management (PRM) 71
P-PRM-01: Allocation of Resources 71
P-PRM-02: Security Requirements Definition 72
P-PRM-03: Secure Development Life Cycle (SDLC) Management 72

Risk Management (RSK) 74
P-RSK-01: Risk Management Program 74
P-RSK-02: Risk Identification 75
P-RSK-03: Risk Assessment 75
P-RSK-04: Risk Remediation 76
P-RSK-05: Business Impact Analysis (BIAs) 77

Secure Engineering & Architecture (SEA) 79
P-SEA-01: Secure Engineering Principles 79
P-SEA-02: Fail Secure 80

Security Awareness & Training (SAT) 81
P-SAT-01: Security & Privacy-Minded Workforce 81
P-SAT-02: Security & Privacy Training 82
P-SAT-03: Privileged Users 83

Technology Development & Acquisition (TDA) 84

P-TDA-01: Separation of Development, Testing & Operational Environments 84

Third-Party Management (TPM) 85
P-TPM-01: Third-Party Management 85
P-TPM-02: Third-Party Criticality Assessments 86
P-TPM-03: Supply Chain Protection 86
P-TPM-04: Third-Party Contract Requirements 87
P-TPM-05: Third-Party Personnel Security 88
P-TPM-06: Third-Party Incident Response & Recovery Capabilities 89

Threat Management (THR) 91
P-THR-01: Threat Awareness Program 91
P-THR-02: Threat Intelligence Feeds 91

Vulnerability & Patch Management (VPM) 93
P-VPM-01: Vulnerability & Patch Management Program 93
P-VPM-02: Continuous Vulnerability Remediation Activities 93
P-VPM-03: Vulnerability Scanning 94
P-VPM-04: Red Team Exercises 95

Glossary: Acronyms & Definitions 97
Acronyms 97
Definitions 97

Record of Changes 98

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.

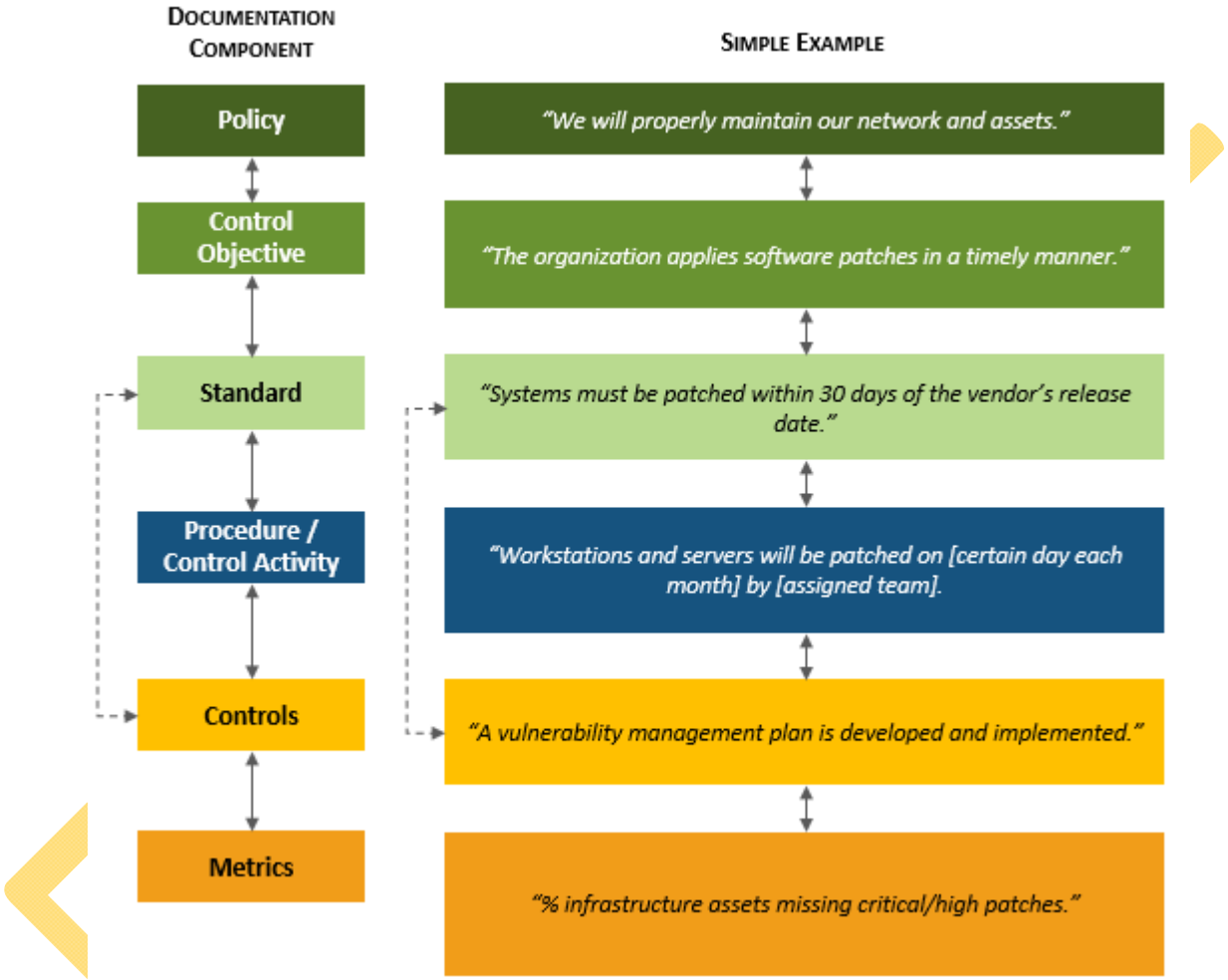
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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

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

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)]*

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]*

[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

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) 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

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

Management Intent: The purpose of the Business Continuity & Disaster Recovery (BCD) policy is to establish processes that will help ACME recover from adverse situations with the minimal impact to operations.

P-BCD-01: CONTINGENCY PLAN

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 develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide Continuity of Operations (COOP) policy, as well as associated standards, controls and procedures.[10]

Control: Mechanisms exist to facilitate the implementation of contingency planning controls.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001], in conjunction with Systems Security Manager [OV-MGT-001], Cyber Defense Infrastructure Support Specialist [PR-INF-001] and Crisis Management Specialist [XX-CON-001] will:

(1) Uses industry-recognized secure practices to develop a contingency plan that:
    a. Identifies essential missions and business functions and associated contingency requirements;
    b. Provides recovery objectives, restoration priorities, and metrics;
    c. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    d. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
    e. Addresses eventual, full system restoration without deterioration of the security measures originally planned and implemented;
    f. Is reviewed and approved by company management; and
    g. Is coordinated with incident handling activities.
(2) Establish procedures for obtaining access to sensitive data during other-than-normal or emergency conditions.
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, review the contingency plan.
(4) 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, request corrective action to address identified deficiencies.
(6) If necessary, validate corrective action occurred to appropriately remediate deficiencies.
(7) If necessary, document the results of corrective action and notes findings.
(8) If necessary, request additional corrective action to address unremediated deficiencies.

P-BCD-02: CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED

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)

[10] NIST 800-53 rev4 PM-8, CP-1 & CP-2 | ISO 27002 17.1.2 | FedRAMP | NIST CSF RC.RP-1 | CCM BCR-01 & BCR-07 | COBIT5 DSS04.01, DSS04.02 & DSS04.03 | ENISA SO19 & SO20 | NISPOM 8-104, 8-603 & 8-614

- 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 incorporates lessons learned for contingency plans.[11]

Control: Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.

Procedure / Control Activity: Crisis Management Specialist [XX-CON-001], in conjunction with Disaster Recovery Team Leader [XX-CON-003] and Business Continuity Team Leader [XX-CON-005]:

(1) Performs a Root Cause Analysis (RCA) following events that trigger usage of continuity plans.
(2) Incorporates lessons learned in updates to the applicable Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, review the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distribute copies of the change to key personnel; and
    b. Communicate the changes and updates to key personnel.
(4) If necessary, request corrective action to address identified deficiencies.
(5) If necessary, validate corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, document the results of corrective action and notes findings.
(7) If necessary, request additional corrective action to address unremediated deficiencies.

P-BCD-03: Contingency Plan Update

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 regularly updates recovery strategies to keep current with business needs and technology changes.[12]

Control: Mechanisms exist to keep contingency plans current with business needs and technology changes.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001], in conjunction with Systems Security Manager [OV-MGT-001], Cyber Defense Infrastructure Support Specialist [PR-INF-001] and Crisis Management Specialist [XX-CON-001] will:

[11] NIST 800-53 rev4 CP-4 | NIST CSF RC.IM-1 | COBIT5 DSS04.05 & DSS04.08 | ENISA SO20 & SO22 | NISPOM 8-615
[12] NIST 800-53 rev4 CP-2 | NIST CSF RC.IM-2 | COBIT5 DSS04.08 | ENISA SO19 & SO20 | NISPOM 8-614

(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.

P-CFG-02: LEAST FUNCTIONALITY

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 configures systems to provide only essential capabilities and specifically prohibits or restricts the use of ports, protocols, and / or services.[20]

Control: Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.

Procedure / Control Activity: System Administrator [OM-ADM-001], in conjunction with Systems Security Analyst [OM-ANA-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure configuration parameters limit privileges to the minimum amount necessary for the user/service to perform needed functions.
(2) Identifies and removes insecure services, protocols, and ports.
(3) Enables only necessary and secure services, protocols, and daemons, as required for the function of the system.
(4) Implements security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.).
(5) Verifies services, protocols, and ports are documented and properly implemented by examining firewall and router configuration settings.
(6) Removes all unnecessary functionality, such as:
    a. Scripts;
    b. Drivers;
    c. Features;
    d. Subsystems;
    e. File systems; and
    f. Unnecessary web servers.
(7) Utilizes network scanning tools, intrusion detection and prevention systems, and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.
(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.

[20] NIST 800-53 rev4 CM-7 & SA-15(5) | FedRAMP | NIST 800-171 3.4.6 | PCI DSS 1.1.5, 1.2.1, 2.2.2, 2.2.4 & 2.2.5 | MA201CMR17 17.03(2)(a) & 17.03(2)(g) | COBIT5 MEA02.03 | | NIST CSF PR.PT-3 | CSC 9.1 | CCM P-IAC-03 | ENISA SO11