YOUR LOGO GOES HERE

# CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

## NIST 800-171 R2

**ACME Consultants, LLP**



SENSITIVE

Access Limited to Authorized Personnel

# Table of Contents


Overview, Instructions & Example 9
Key Terminology 9
Overview 9
*Customization Guidance* 9
*Validating Needs for Procedures / Control Activities* 9
Procedures Documentation 10
NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework 11
Example 11
Supporting Policies & Standards 14
Policies, Controls, Standards, Procedures & Guidelines Structure 14
Security, Compliance & Resilience Governance (GOV) Procedures 15
P-GOV-01: NIST 800-171 Compliance Program (NCP) 15
P-GOV-02: Publishing Security, Compliance & Resilience Documentation 15
P-GOV-04: Assigned Security, Compliance & Resilience Responsibilities 16
*P-GOV-04.1: Assigned Security, Compliance & Resilience Responsibilities | Accountability Structure* 16
P-GOV-15: Operationalizing Security, Compliance & Resilience Practices 17
*P-GOV-15.1: Operationalizing Security, Compliance & Resilience Practices | Select Controls* 17
*P-GOV-15.2: Operationalizing Security, Compliance & Resilience Practices | Implement Controls* 18
*P-GOV-15.3: Operationalizing Security, Compliance & Resilience Practices | Assess Controls* 18
*P-GOV-15.4: Operationalizing Security, Compliance & Resilience Practices | Authorize Technology Assets, Applications and/or Services (TAAS)* 18
*P-GOV-15.5: Operationalizing Security, Compliance & Resilience Practices | Monitor Controls* 19
P-GOV-17: Security, Compliance & Resilience Status Reporting 20
Asset Management (AST) Procedures 21
P-AST-01: Asset Governance 21
P-AST-02: Asset Inventories 21
*P-AST-02.1: Asset Inventories | Updates During Installations/Removals* 22
*P-AST-02.3: Asset Inventories | Component Duplication Avoidance* 22
P-AST-05: Security of Assets & Media 22
P-AST-09: Secure Disposal, Destruction or Re-Use of Equipment 23
P-AST-17: Prohibited Equipment & Services 23
Business Continuity & Disaster Recovery (BCD) Procedures 25
P-BCD-01: Business Continuity Management System (BCMS) 25
P-BCD-11: Data Backups 25
*P-BCD-11.4: Data Backups | Cryptographic Protection* 26
Change Management (CHG) Procedures 27
P-CHG-01: Change Management Program 27
P-CHG-02: Configuration Change Control 27
*P-CHG-02.2: Configuration Change Control | Test, Validate & Document Changes* 28
P-CHG-03: Security Impact Analysis for Changes 29
P-CHG-04: Access Restriction For Change 29
*P-CHG-04.1: Access Restrictions For Change | Automated Access Enforcement/Auditing* 30
P-CHG-05: Stakeholder Notification of Changes 30
Cloud Security (CLD) Procedures 31
P-CLD-01: Cloud Services 31
P-CLD-02: Cloud Security Architecture 31
P-CLD-03: Cloud Infrastructure Security Subnet 32
P-CLD-06: Multi-Tenant Environments 32
P-CLD-10: Sensitive Data In Public Cloud Providers 33
Compliance (CPL) Procedures 34
P-CPL-01: Statutory, Regulatory & Contractual Compliance 34
*P-CPL-01.7: Statutory, Regulatory & Contractual Compliance | Designated Certifying Official* 34
*P-CPL-01.8: Statutory, Regulatory & Contractual Compliance | Conformity Attestations* 35
P-CPL-02: Security, Compliance & Resilience Controls Oversight 35
*P-CPL-02.1: Security, Compliance & Resilience Controls Oversight | Internal Audit Function* 36

**P-CPL-03: Security, Compliance & Resilience Assessments** 37
*P-CPL-03.1: Security, Compliance & Resilience Assessments | Independent Assessors* 38
**Configuration Management (CFG) Procedures** 39
**P-CFG-01: Configuration Management Program** 39
**P-CFG-02: Secure Baseline Configurations** 39
*P-CFG-02.1: System Hardening Through Baseline Configurations | Reviews & Updates* 41
*P-CFG-02.5: Secure Baseline Configurations | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas* 42
*P-CFG-02.9: Secure Baseline Configurations | Baseline Tailoring* 43
**P-CFG-03: Least Functionality** 44
*P-CFG-03.1: Least Functionality | Periodic Review* 45
*P-CFG-03.2: Least Functionality | Prevent Unauthorized Software Execution* 45
*P-CFG-03.3: Least Functionality | Explicitly Allow / Deny Applications* 46
*P-CFG-03.4: Least Functionality | Split Tunneling* 46
**P-CFG-05: User-Installed Software** 46
**Continuous Monitoring (MON) Procedures** 48
**P-MON-01: Continuous Monitoring** 48
*P-MON-01.3: Continuous Monitoring | Inbound & Outbound Communications Traffic* 49
*P-MON-01.4: Continuous Monitoring | System Generated Alerts* 50
*P-MON-01.8: Continuous Monitoring | Security Event Monitoring* 51
*P-MON-01.16: Continuous Monitoring | Analyze & Prioritize Monitoring Requirements* 52
**P-MON-02: Centralized Event Log Collection** 53
*P-MON-02.1: Centralized Security Event Log Collection | Correlate Monitoring Information* 55
**P-MON-03: Content of Event Logs** 55
*P-MON-03.1: Content Of Event Logs | Sensitive Event Log Information* 56
*P-MON-03.2: Content Of Event Logs | Audit Trails* 57
*P-MON-03.7: Content Of Event Logs | Database Logging* 57
**P-MON-05: Response To Event Log Processing Failures** 58
**P-MON-06: Monitoring Reporting** 58
**P-MON-07: Time Stamps** 59
*P-MON-07.1: Time Stamps | Synchronization With Authoritative Time Source* 59
**P-MON-08: Protection of Event Logs** 60
*P-MON-08.2: Protection of Event Logs | Access by Subset of Privileged Users* 61
**P-MON-09: Non-Repudiation** 61
*P-MON-09.1: Non-Repudiation | Identity Binding* 62
**P-MON-10: Event Log Retention** 62
**P-MON-11: Monitoring For Information Disclosure** 62
*P-MON-11.3: Monitoring For Information Disclosure | Monitoring for Indicators of Compromise (IOC)* 63
**P-MON-16: Anomalous Behavior** 63
**Cryptographic Protections (CRY) Procedures** 65
**P-CRY-01: Use of Cryptographic Controls** 65
*P-CRY-01.1: Use of Cryptographic Controls | Alternate Physical Protection* 66
**P-CRY-03: Transmission Confidentiality** 66
**P-CRY-04: Transmission Integrity** 67
**P-CRY-05: Encrypting Data At Rest** 67
**P-CRY-08: Public Key Infrastructure (PKI)** 68
**P-CRY-09: Cryptographic Key Management** 68
**Data Classification & Handling (DCH) Procedures** 70
**P-DCH-01: Data Protection** 70
*P-DCH-01.2: Data Protection | Sensitive/Regulated Data Protection* 70
**P-DCH-03: Media Access** 70
**P-DCH-04: Media Marking** 71
**P-DCH-06: Media Storage** 72
**P-DCH-07: Media Transportation** 73
**P-DCH-08: Physical Medial Disposal** 73
**P-DCH-09: System Media Sanitization** 74
**P-DCH-10: Media Use** 75

*P-DCH-10.2: Media Use | Prohibit Use Without Owner* 75
**P-DCH-13: Use of External Technology Assets, Applications and/or Services (TAAS)** 75
*P-DCH-13.1: Use of External Technology Assets, Applications and/or Services (TAAS) | Limits of Authorized Use* 76
*P-DCH-13.2: Use of External Technology Assets, Applications and/or Services (TAAS) | Portable Storage Devices* 77
**P-DCH-15: Publicly Accessible Content** 77
**P-DCH-17: Ad-Hoc Transfers** 78
**Endpoint Security (END) Procedures** 80
**P-END-01: Endpoint Device Management (EDM)** 80
**P-END-02: Unified Endpoint Device Management (UEDM)** 80
**P-END-03: Prohibit Installation Without Privileged Status** 81
*P-END-03.2: Prohibit Installation Without Privileged Status | Governing Access Restriction for Change* 82
**P-END-04: Malicious Code Protection (Anti-Malware)** 82
*P-END-04.1: Malicious Code Protection (Anti-malware) | Automatic Antimalware Signature Updates* 83
*P-END-04.7: Malicious Code Protection (Anti-malware) | Always On Protection* 83
**P-END-10: Mobile Code** 84
**P-END-14: Collaborative Computing Devices** 85
**Human Resources Security (HRS) Procedures** 87
**P-HRS-01: Human Resources Security Management** 87
*P-HRS-01.1: Human Resources Security Management | Onboarding, Transferring & Offboarding Personnel* 88
**P-HRS-04: Personnel Screening** 89
*P-HRS-04.1: Personnel Screening | Roles With Special Protection Measures* 90
*P-HRS-04.2: Personnel Screening | Formal Indoctrination* 90
**P-HRS-05: Terms of Employment** 91
*P-HRS-05.1: Terms of Employment | Rules of Behavior* 91
*P-HRS-05.2: Terms of Employment | Social Media & Social Networking Restrictions* 92
**P-HRS-06: Access Agreements** 93
**P-HRS-07: Personnel Sanctions** 93
**P-HRS-08: Personnel Transfer** 94
**P-HRS-09: Personnel Termination** 94
**P-HRS-10: Third-Party Personnel** 95
**P-HRS-11: Separation of Duties (SoD)** 96
**Identification & Authentication (IAC) Procedures** 97
**P-IAC-01: Identity & Access Management (IAM)** 97
**P-IAC-02: Identification & Authentication for Organizational Users** 97
*P-IAC-02.2: Identification & Authentication for Organizational Users | Replay-Resistant Authentication* 98
**P-IAC-04: Identification & Authentication for Devices** 98
**P-IAC-06: Multi-Factor Authentication (MFA)** 99
*P-IAC-06.1: Multi-Factor Authentication (MFA) | Network Access to Privileged Accounts* 99
*P-IAC-06.2: Multi-Factor Authentication (MFA) | Network Access to Non-Privileged Accounts* 100
*P-IAC-06.3: Multi-Factor Authentication (MFA) | Local Access to Privileged Accounts* 100
**P-IAC-08: Role-Based Access Control (RBAC)** 101
**P-IAC-09: Identifier Management (User Names)** 101
*P-IAC-09.5: Identifier Management | Privileged Account Identifiers* 103
**P-IAC-10: Authenticator Management** 104
*P-IAC-10.1: Authenticator Management | Password-Based Authentication* 105
*P-IAC-10.5: Authenticator Management | Protection of Authenticators* 107
**P-IAC-11: Authenticator Feedback** 107
**P-IAC-15: Account Management** 108
*P-IAC-15.1: Account Management | Automated System Account Management (Directory Services)* 110
*P-IAC-15.3: Account Management | Disable Inactive Accounts* 110
**P-IAC-16: Privileged Account Management (PAM)** 111
*P-IAC-16.1: Privileged Account Management (PAM) | Privileged Account Inventories* 112
**P-IAC-20: Access Enforcement** 112
**P-IAC-21: Least Privilege** 114
*P-IAC-21.1: Least Privilege | Authorize Access to Security Functions* 114
*P-IAC-21.2: Least Privilege | Non-Privileged Access for Non-Security Functions* 115
*P-IAC-21.3: Least Privilege | Management Approval For Privileged Accounts* 116

*P-IAC-21.4: Least Privilege | Auditing Use of Privileged Functions* 116
*P-IAC-21.5: Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions* 117
**P-IAC-22: Account Lockout** 117
**P-IAC-24: Session Lock** 118
*P-IAC-24.1: Session Lock | Pattern-Hiding Displays* 118
**P-IAC-25: Session Termination** 119
**Incident Response (IRO) Procedures** 120
**P-IRO-01: Incidents Response Operations** 120
**P-IRO-02: Incident Handling** 120
**P-IRO-03: Indicators of Compromise (IOC)** 121
**P-IRO-04: Incident Response Plan (IRP)** 121
*P-IRO-04.2: Incident Response Plan (IRP) | IRP Update* 122
**P-IRO-05: Incident Response Training** 123
**P-IRO-06: Incident Response Testing** 123
**P-IRO-08: Chain of Custody & Forensics** 124
**P-IRO-10: Incident Stakeholder Reporting** 124
*P-IRO-10.2: Incident Stakeholder Reporting | Cyber Incident Reporting for Sensitive / Regulated Data* 125
**P-IRO-11: Incident Reporting Assistance** 126
*P-IRO-11.2: Incident Reporting Assistance | Coordination With External Providers* 126
**P-IRO-12: Sensitive / Regulated Data Spill Response** 127
*P-IRO-12.1: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Spill Responsible Personnel* 127
*P-IRO-12.2: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Spill Training* 127
*P-IRO-12.3: Sensitive / Regulated Data Spill Response | Post-Sensitive / Regulated Data Spill Operations* 128
*P-IRO-12.4: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Exposure to Unauthorized Personnel* 128
**P-IRO-13: Root Cause Analysis (RCA) & Lessons Learned** 129
**Information Assurance (IAO) Procedures** 130
**P-IAO-01: Information Assurance (IA) Operations** 130
*P-IAO-01.1: Information Assurance (IA) Operations | Assessment Boundaries* 130
**P-IAO-02: Assessments** 131
*P-IAO-02.1: Assessments | Independent Assessors* 132
**P-IAO-03: Applied Security, Compliance and Resilience Controls Documentation [System Security Plan (SSP)]** 132
*P-IAO-03.1: Applied Security, Compliance and Resilience Controls Documentation | Plan/Coordinate with Other Organizational Entities* 134
*P-IAO-03.2: Applied Security, Compliance and Resilience Controls Documentation | Adequate Security for Sensitive / Regulated Data In Support of Contracts* 135
**P-IAO-05: Capabilities Deficiency Tracking [Plan of Action and Milestones (POA&M)]** 136
**Maintenance (MNT) Procedures** 138
**P-MNT-01: Maintenance Operations** 138
**P-MNT-02: Controlled Maintenance** 138
**P-MNT-04: Maintenance Tools** 139
*P-MNT-04.2: Maintenance Tools | Inspect Media* 139
**P-MNT-05: Remote Maintenance** 140
*P-MNT-05.2: Remote Maintenance | Remote Maintenance Notifications* 140
*P-MNT-05.4: Remote Maintenance | Remote Maintenance Disconnect Verification* 140
**P-MNT-06: Maintenance Personnel** 141
*P-MNT-06.1: Maintenance Personnel | Maintenance Personnel Without Appropriate Access* 141
*P-MNT-06.2: Maintenance Personnel | Non-System Related Maintenance* 142
**Mobile Device Management (MDM) Procedures** 143
**P-MDM-01: Centralized Management Of Mobile Devices** 143
**P-MDM-02: Access Control For Mobile Devices** 143
**P-MDM-03: Full Device & Container-Based Encryption** 144
**P-MDM-06: Personally-Owned Mobile Devices** 145
**P-MDM-07: Organization-Owned Mobile Devices** 146
**Network Security (NET) Procedures** 147
**P-NET-01: Network Security Controls (NSC)** 147

**P-NET-02: Layered Defenses** 147
*P-NET-02.2: Layered Defenses | Guest Networks* 148
**P-NET-03: Boundary Protection** 148
*P-NET-03.1: Boundary Protection | Limit Network Connections* 150
*P-NET-03.2: Boundary Protection | External Telecommunications Services* 150
**P-NET-04: Data Flow Enforcement – Access Control Lists (ACLs)** 150
*P-NET-04.1: Data Flow Enforcement | Deny Traffic by Default & Allow Traffic by Exception* 151
**P-NET-05: Interconnection Security Agreements (ISAs)** 152
*P-NET-05.2: Interconnection Security Agreements (ISAs) | Internal System Connections* 153
**P-NET-06: Network Segmentation (macrosegmentation)** 153
**P-NET-07: Network Connection Termination** 154
**P-NET-08: Network Intrusion Detection & Prevention Systems (NIDS/NIPS)** 155
**P-NET-09: Session Integrity** 155
**P-NET-10: Domain Name Service (DNS) Resolution** 156
*P-NET-10.1: Domain Name Service (DNS) Resolution | Architecture & Provisioning For Name/Address Resolution Service* 156
*P-NET-10.2: Domain Name Service (DNS) Resolution | Secure Name/Address Resolution Service (Recursive or Caching Resolver)* 157
**P-NET-13: Electronic Messaging** 157
**P-NET-14: Remote Access** 157
*P-NET-14.1: Remote Access | Automated Monitoring & Control* 158
*P-NET-14.2: Remote Access | Protection of Confidentiality/Integrity Using Encryption* 158
*P-NET-14.3: Remote Access | Managed Access Control Points* 159
*P-NET-14.4: Remote Access | Privileged Commands & Access* 159
*P-NET-14.5: Remote Access | Work From Anywhere (WFA) – Telecommuting Security* 160
**P-NET-15: Wireless Networking** 161
*P-NET-15.1: Wireless Access | Authentication & Encryption* 161
**P-NET-18: DNS & Content Filtering** 162
**Physical & Environmental Security (PES) Procedure** 163
**P-PES-01: Physical & Environmental Protections** 163
**P-PES-02: Physical Access Authorizations** 163
*P-PES-02.1: Physical Access Authorizations | Role-Based Physical Access* 164
**P-PES-03: Physical Access Control** 164
*P-PES-03.3: Physical Access Control | Physical Access Logs* 166
*P-PES-03.4: Physical Access Control | Access To Critical Systems* 166
**P-PES-04: Physical Security of Offices, Rooms & Facilities** 167
**P-PES-05: Monitoring Physical Access** 167
*P-PES-05.1: Monitoring Physical Access | Intrusion Alarms/Surveillance Equipment* 168
*P-PES-05.2: Monitoring Physical Access | Monitoring Physical Access To Critical Systems* 168
**P-PES-06: Visitor Control** 169
*P-PES-06.1: Visitor Control | Distinguish Visitors from On-Site Personnel* 170
*P-PES-06.3: Visitor Control | Restrict Unescorted Access* 170
**P-PES-10: Delivery & Removal** 171
**P-PES-11: Alternate Work Site** 171
**P-PES-12: Equipment Siting & Protection** 172
*P-PES-12.1: Equipment Siting & Protection | Transmission Medium Security* 173
*P-PES-12.2: Equipment Siting & Protection | Access Control For Output Devices* 173
**Project & Resource Management (PRM) Procedures** 175
**P-PRM-01: Security, Compliance & Resilience Portfolio Management** 175
**P-PRM-03: Allocation of Resources** 175
**P-PRM-07: System Development Life Cycle (SDLC) Management** 176
**Risk Management (RSK) Procedures** 177
**P-RSK-01: Risk Management Program (RMP)** 177
**P-RSK-04: Risk Assessment** 177
**P-RSK-06: Risk Remediation** 178
*P-RSK-06.2: Risk Remediation | Compensating Countermeasures* 179
**Secure Engineering & Architecture (SEA) Procedure** 180

**P-SEA-01: Secure Engineering Principles** 180
**P-SEA-02: Alignment With Enterprise Architecture** 181
*P-SEA-02.1: Alignment With Enterprise Architecture | Standardized Terminology* 181
**P-SEA-03: Defense-In-Depth (DiD) Architecture** 182
*P-SEA-03.2: Defense-In-Depth (DiD) Architecture | Application Partitioning* 182
**P-SEA-04: Process Isolation** 183
**P-SEA-05: Information In Shared Resources** 183
**P-SEA-07: Predictable Failure Analysis** 184
*P-SEA-07.1: Predictable Failure Analysis | Technology Lifecycle Management* 184
**P-SEA-10: Memory Protection** 185
**P-SEA-18: System Use Notification (Logon Banner)** 185
*P-SEA-18.1: System Use Notification | Standardized Microsoft Windows Banner* 185
*P-SEA-18.2: System Use Notification | Truncated Banner* 186
**P-SEA-20: Clock Synchronization** 187

**Security Awareness & Training (SAT) Procedures** 188
**P-SAT-01: Security, Compliance & Resilience-Minded Workforce** 188
**P-SAT-02: Security, Compliance & Resilience Awareness Training** 188
**P-SAT-03: Security, Compliance & Resilience Role-Based Training** 190
*P-SAT-03.6: Security, Compliance & Resilience Training | Cyber Threat Environment* 191
**P-SAT-04: Security, Compliance & Resilience Training Records** 191

**Technology Development & Acquisition (TDA) Procedures** 193
**P-TDA-01: Technology Development & Acquisition** 193
**P-TDA-02: Minimum Viable Product (MVP) Security Requirements** 193
*P-TDA-02.1: Minimum Viable Product (MVP) Security Requirements | Ports, Protocols & Services In Use* 194
*P-TDA-02.2: Minimum Viable Product (MVP) Security Requirements | Information Assurance Enabled Products* 194
**P-TDA-04: Documentation Requirements** 194
*P-TDA-04.1: Documentation Requirements | Functional Properties* 195
**P-TDA-06: Secure Software Development Practices (SSDP)** 196
**P-TDA-08: Separation of Development, Testing & Operational Environments** 197
**P-TDA-09: Security, Compliance & Resilience Testing Throughout Development** 198
**P-TDA-14: Developer Configuration Management** 198

**Third-Party Management (TPM) Procedures** 200
**P-TPM-01: Third-Party Management** 200
**P-TPM-04: Third-Party Services** 200
*P-TPM-04.2: Third-Party Services | External Connectivity Requirements - Identification of Ports, Protocols & Services* 201
**P-TPM-05: Third-Party Contract Requirements** 201
*P-TPM-05.2: Third-Party Contract Requirements | Contract Flow-Down Requirements* 202

**Threat Management (THR) Procedures** 204
**P-THR-01: Threat Awareness Program** 204
**P-THR-03: Threat Intelligence Feeds** 204
**P-THR-05: Insider Threat Awareness** 205

**Vulnerability & Patch Management (VPM) Procedures** 206
**P-VPM-01: Vulnerability & Patch Management Program** 206
**P-VPM-02: Vulnerability Remediation Process** 206
**P-VPM-04: Continuous Vulnerability Remediation Activities** 207
**P-VPM-05: Software & Firmware Patching** 207
**P-VPM-06: Vulnerability Scanning** 209
*P-VPM-06.1: Vulnerability Scanning | Update Tool Capability* 210
*P-VPM-06.3: Vulnerability Scanning | Privileged Access* 211

**Web Security (WEB) Procedures** 212
**P-WEB-01: Web Security** 212
**P-WEB-02: Use of Demilitarized Zones (DMZs)** 212
**P-WEB-04: Client-Facing Web Services** 213

**Glossary: Acronyms & Definitions** 214
**Acronyms** 214

DEFINITIONS 215
RECORD OF CHANGES 216

## KEY TERMINOLOGY

With the Cybersecurity Standardized Operating Procedures (CSOP), it is important to understand a few key terms:

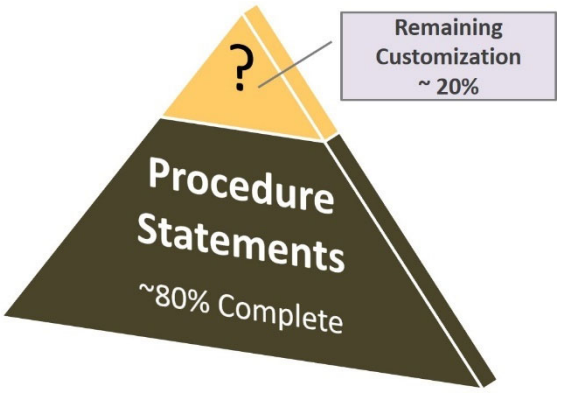
- Procedure / Control Activity: Procedures represent an established way of doing something, such as a series of actions conducted in a specified order or manner. Some organizations refer to procedures as "control activities" and the terms essentially synonymous. In the CSOP, the terms procedure or control 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.

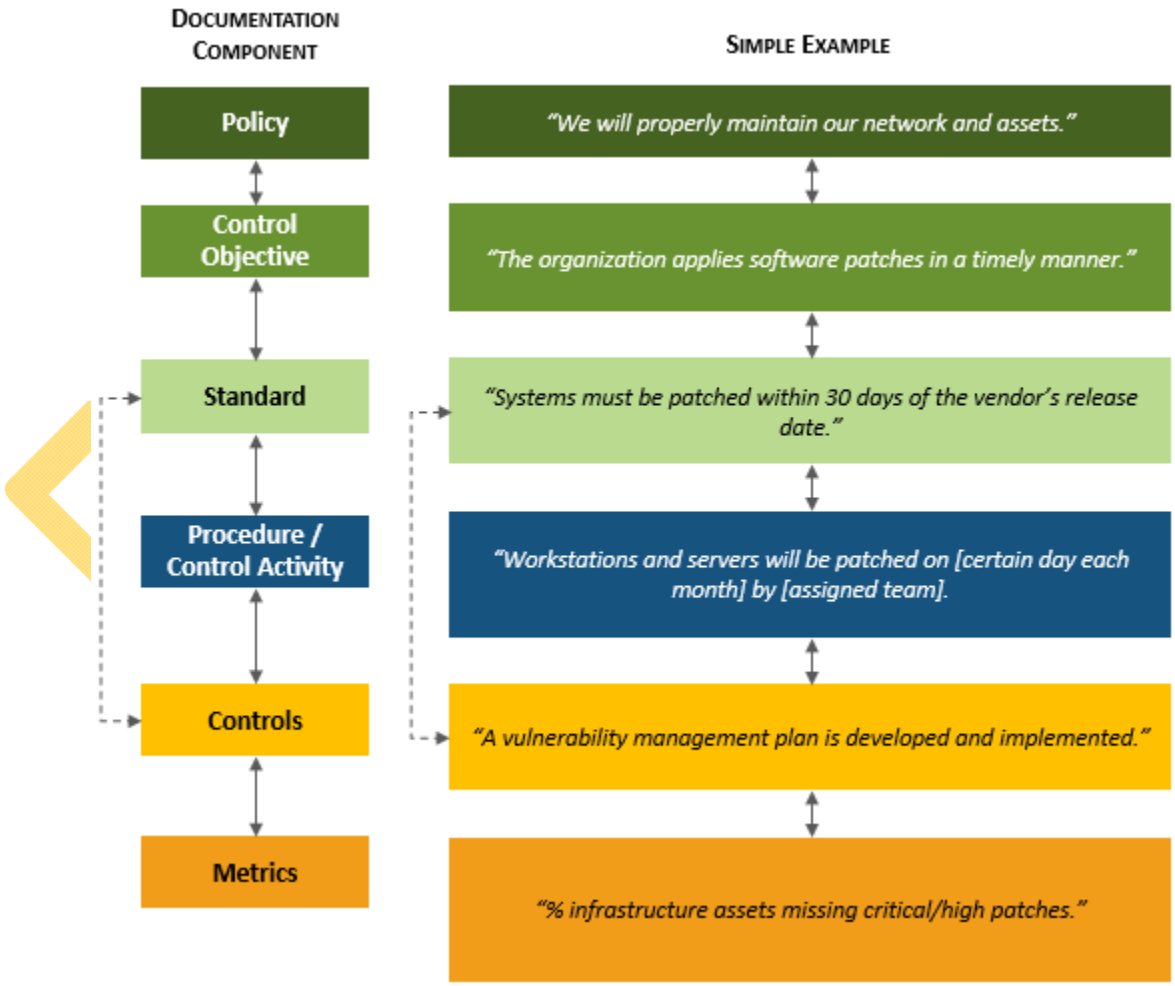
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

From a due care and due diligence perspective, it can be thought of this way:

- Certain standards require processes to exist *(due diligence – evidence demonstrates standards exist)*.
- Performing the activities outlined in a procedure and documenting the work that was performed satisfies the intent of the standard *(due care – evidence demonstrates the standard is operating effectively)*.

The diagram shown below helps visualize the linkages in documentation that involve written procedures:

- CONTROL OBJECTIVES exist to support POLICIES;
- STANDARDS are written to support CONTROL OBJECTIVES;
- PROCEDURES are written to implement the requirements that STANDARDS establish;
- CONTROLS exist as a mechanism to assess/audit both the existence of PROCEDURES / STANDARDS and how well their capabilities are implemented and/or functioning; and
- METRICS exist as a way to measure the performance of CONTROLS.



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

The CSOP leverages the NIST NICE Cybersecurity Workforce Framework.[1] The purpose of this framework is that work roles have an impact on an organization's ability to protect its data, systems and operations. By assigning work roles, it helps direct the work of employees and contractors to minimize assumptions about who is responsible for certain security, compliance and resilience 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 v2.0.0 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 assigned 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/nice-framework-resource-center*

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]
    a. Includes hardware, software and firmware in baseline configurations. [3]
    b. Where technically feasible, technology platforms align with reasonably-expected hardening practices that apply the appropriate use of common security configurations available from the National Institute of Standards and Technology's National Checklist Program (NCP) website:[4]
        i. Center for Internet Security (CIS) benchmarks;[5]
        ii. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs);[6]or
        iii. Original Equipment Manufacturer (OEM) security configuration guidance.

(2) Technology platforms that include, but are not limited to:
    a. Server-Class Systems
        i. Microsoft Server 2016
        ii. Microsoft Server 2018
        iii. Microsoft Server 2020
        iv. Microsoft Server 2022
        v. Red Hat Enterprise Linux (RHEL)
        vi. Unix
        vii. Solaris
    b. Workstation-Class Systems
        i. Microsoft 10
        ii. Microsoft 11
        iii. Apple
        iv. Fedora (Linux)
        v. Ubuntu (Linux)
        vi. 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



---

[2] *NIST SP 800-171A / CMMC 2.0: 3.4.1[a], 3.4.1[c], 3.4.2[a] & 3.4.2[b] / CM.L2-3.4.1[a], CM.L2-3.4.1[c], CM.L2-3.4.2[a] & CM.L2-3.4.2[b]*
[3] *NIST SP 800-171A / CMMC 2.0: 3.4.1[b] / CM.L2-3.4.1[b] | NIST SP 800-171A R3: A.03.01.03[01], A.03.01.16.a[03], A.03.01.16.c, A.03.01.18.a[02], A.03.03.08.a[02], A.03.04.01.a[01], A.03.04.01.a[02], A.03.04.02.a[01], A.03.04.02.a[02], A.03.04.06.b[01], A.03.04.06.b[02], A.03.04.06.b[03], A.03.04.06.b[04], A.03.04.06.b[05], A.03.04.06.ODP[01], A.03.04.06.ODP[02], A.03.04.06.ODP[03], A.03.04.06.ODP[04], A.03.04.06.ODP[05], A.03.05.04[01], A.03.05.04[02], A.03.05.07.c, A.03.05.07.d, A.03.05.07.e, A.03.05.07.f, A.03.07.05.b[02]*
[4] *NIST NCP website - https://ncp.nist.gov/repository*
[5] *CIS Benchmarks - https://www.cisecurity.org/cis-benchmarks/*
[6] *DISA STIGs official site - https://public.cyber.mil/stigs/*

ii. Windows SQL Server
iii. Windows SQL Express
iv. Oracle
v. DB2

(3) Ensures that system hardening includes, but is not limited to the following criteria:
   a. Each Operating System (OS) must:
      i. Be hardened to provide only necessary functionality (e.g., ports, protocols, services, etc.) to meet business needs;
      ii. Prevent remote devices from simultaneously establishing nonremote connections with organizational systems and communicating via some other unauthorized connection to resources in external networks (e.g., split tunneling); and
      iii. Include necessary technology controls that are required for the secure use of the OS in a production environment (e.g., antimalware, event log forwarding, content filtering, etc.);
   b. Deviations from secure baseline configurations must be:
      i. Approved in accordance with ACME's change management processes, prior to deployment, provisioning or use;[7] and
      ii. Authorized following change management processes prior to deployment, provisioning or use.
   c. 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.
   d. Configuring and documenting only the necessary ports, protocols and services to meet business needs;
   e. 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;
   f. 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
   g. 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) 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.
(6) 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.
(7) If necessary, requests corrective action to address identified deficiencies.
(8) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(9) If necessary, documents the results of corrective action and notes findings.
(10) If necessary, requests additional corrective action to address unremediated deficiencies.

[7] *NIST SP 800-171A R3: A.03.04.02.b[01], A.03.04.02.b[02]*

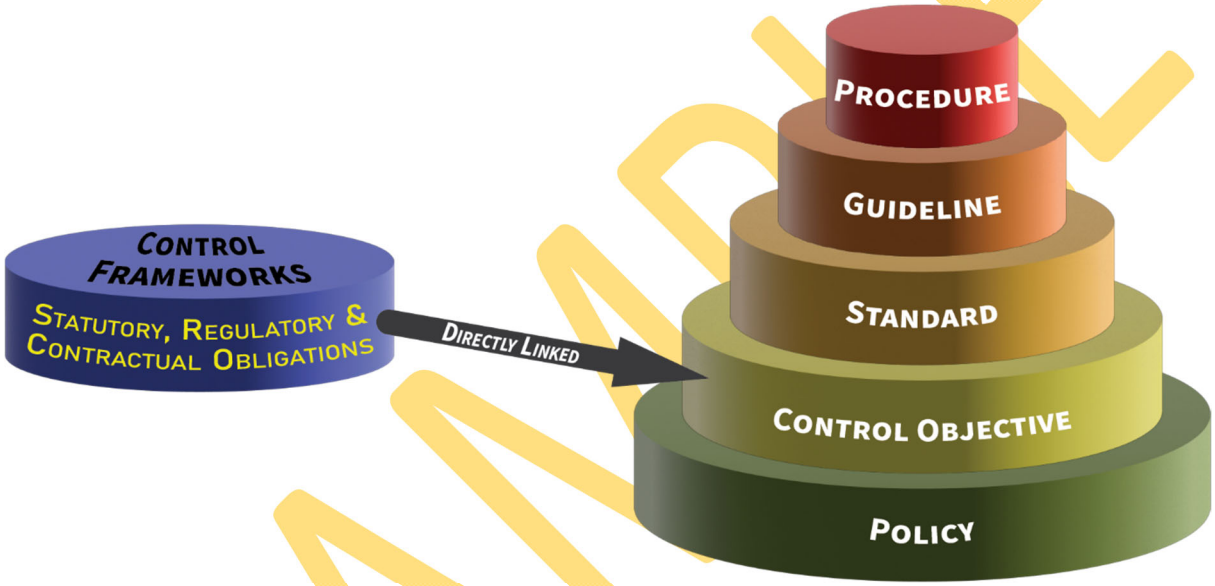
## Supporting Policies & Standards

While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with NIST 800-171 Compliance Program (NCP) that contains policies, control objectives, standards and guidelines.

## Policies, Controls, Standards, Procedures & Guidelines Structure

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

(1) Policy that establishes management's intent;
(2) Control Objective that identifies leading practices (linked to controls);
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.



Management Intent: The purpose of the Asset Management (AST) procedures / control activities is to ensure that Technology Assets, Applications and/or Services (TAAS) are properly managed throughout the lifecycle of the asset, from procurement through disposal.

## P-AST-01: ASSET GOVERNANCE

Control: Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.

Procedure / Control Activity: IT Asset Management (ITAM) Manager [IO-ORG-001], in conjunction with Asset Owner [OG-ORG-007]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to maintain current inventories of ACME's Technology Assets, Applications and/or Services (TAAS) that includes, but is not limited to:
    a. A list of all such devices and personnel with access;
    b. A method to accurately and readily determine owner, contact information, and purpose (e.g., labeling, coding, and/or inventorying of devices); and
    c. A list of company-approved products.
(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, IT Asset Management (ITAM) Manager [IO-ORG-001], in conjunction with Asset Owner [OG-ORG-007], 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-AST-02: ASSET INVENTORIES

Control: Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:

(1) Accurately reflects the current TAASD in use;
(2) Identifies authorized software products, including business justification details;
(3) Is at the level of granularity deemed necessary for tracking and reporting;
(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and
(5) Is available for review and audit by designated organizational personnel.

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

(1) Maintains an inventory of Technology Assets, Applications, Services and/or Data (TAASD) that includes, but is not limited to: [14]
    a. Hardware and software inventories, both:
        i. Internally-hosted assets; and
        ii. Externally-hosted assets; and
    b. A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding, and/or inventorying of devices).
(2) Assigns one of the following classifications to each Technology Asset, Application and/or Service (TAAS), per CMMC scoping guidelines:
    a. CUI Asset;
    b. Security Protection Asset (SPA);
    c. Contractor Risk Managed Asset (CRMA)
    d. Specialized Asset (SA); or

[14] *NIST SP 800-171A / CMMC 2.0: 3.4.1[d], 3.4.1[e] & 3.4.1[f] / CM.L2-3.4.1[d], CM.L2-3.4.1[e] & CM.L2-3.4.1[f] | NIST SP 800-171A R3: A.03.04.10.a*

e. Out of Scope Asset (OSA);

(3) On at least a quarterly basis, updates the inventory. [15]

(4) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the asset inventory 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-AST-02.1: ASSET INVENTORIES | UPDATES DURING INSTALLATIONS/REMOVALS**

Control: Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.

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

(1) Updates the system inventory after component installations, removals, and system updates. [16]

(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-AST-02.3: ASSET INVENTORIES | COMPONENT DUPLICATION AVOIDANCE**

Control: Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.

Procedure / Control Activity: Systems Administration [IO-WRL-005], in conjunction with Asset Owner [OG-ORG-007] and IT Asset Management (ITAM) Manager [IO-ORG-001]:

(1) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, [process operator] reviews in-scope assets and verifies that system components are not duplicated in other asset inventories.

(2) As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:

a. Distributes copies of the change to key personnel; and

b. Communicates the changes and updates to key personnel.

(3) If necessary, requests corrective action to address identified deficiencies.

(4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.

(5) If necessary, documents the results of corrective action and notes findings.

(6) If necessary, requests additional corrective action to address unremediated deficiencies.

## P-AST-05: SECURITY OF ASSETS & MEDIA

Control: Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.

Procedure / Control Activity: IT Asset Management (ITAM) Manager [IO-ORG-001], in conjunction with Asset Owner [OG-ORG-007], Systems Administration [IO-WRL-005] and Secure Systems Development [DD-WRL-004]:

(1) Implements appropriate administrative and technical means to ensure asset custodians and data / process owners maintain strict control over the internal or external distribution of assets or media, including the following:

---

[15] *NIST SP 800-171A R3: A.03.04.10.b[01], A.03.04.10.b[02], NIST SP 800-171A R3: A.03.04.10.ODP[01]*

[16] *NIST SP 800-171A R3: A.03.04.10.c[01], A.03.04.10.c[02], A.03.04.10.c[03]*

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:[20]
    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; [21]
    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; [22]
        ii. Reviewed; [23]
        iii. Approved or Disapproved; [24]and
        iv. Documented. [25]

[20] *NIST SP 800-171A R3: A.03.04.03.d[01]*
[21] *NIST SP 800-171A R3: A.03.04.03.d[02]*
[22] *NIST SP 800-171A / CMMC 2.0: 3.4.3[a] / CM.L2-3.4.3[a]*
[23] *NIST SP 800-171A / CMMC 2.0: 3.4.3[b] / CM.L2-3.4.3[b]*
[24] *NIST SP 800-171A / CMMC 2.0: 3.4.3[c] / CM.L2-3.4.3[c]*
[25] *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:[26]
    a. Preventative maintenance of production Technology Assets, Applications and/or Services (TAAS);
    b. Reactive / emergency maintenance of production TAAS;
    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 TAAS.[27]
(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-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 [IO-ORG-002]:

(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 Technology Assets, Applications and/or Services (TAAS) 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) Document the changes that were implemented in the production environment. [28]
(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.

[26] *NIST SP 800-171A R3: A.03.04.03.a*
[27] *NIST SP 800-171A R3: A.03.04.03.c[01]*
[28] *NIST SP 800-171A R3: A.03.04.03.c[02]*