

YOUR LOGO GOES HERE

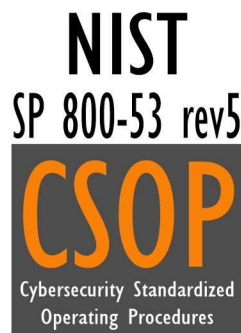
---

# CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

---

*[NIST SP 800 53 REV5 – LOW & MODERATE BASELINES]*

**ACME Consulting Services, LLP**



**INTERNAL USE**

Access Limited to Internal Use Only

***IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES  
WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)***

## TABLE OF CONTENTS

<b>OVERVIEW, INSTRUCTIONS &amp; EXAMPLE</b>	<b>11</b>
<b>KEY TERMINOLOGY</b>	<b>11</b>
<b>OVERVIEW</b>	<b>11</b>
Customization Guidance	11
Validating Needs for Procedures / Control Activities	11
<b>UNDERSTANDING CONTROL OBJECTIVES &amp; CONTROLS</b>	<b>11</b>
<b>PROCEDURES DOCUMENTATION</b>	<b>12</b>
NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	13
Example Procedure	13
Supporting Policies & Standards	16
<b>KNOWN COMPLIANCE REQUIREMENTS</b>	<b>18</b>
<b>STATUTORY REQUIREMENTS</b>	<b>18</b>
<b>REGULATORY REQUIREMENTS</b>	<b>18</b>
<b>CONTRACTUAL REQUIREMENTS</b>	<b>18</b>
<b>MANAGEMENT CONTROLS</b>	<b>19</b>
<b>PROGRAM MANAGEMENT (PM)</b>	<b>19</b>
P-PM-1: Information Security Program Plan	19
P-PM-2: Information Security Program Leadership Role	20
P-PM-3: Information Security and Privacy Resources	20
P-PM-4: Plan of Action & Milestones (POA&M) Process (Vulnerability Remediation)	21
P-PM-5: System Inventory	22
<i>PM-5(1): System Inventory   Inventory of Personally Identifiable Information (PII)</i>	23
P-PM-6: Measures of Performance (Metrics)	23
P-PM-7: Enterprise Architecture	24
<i>P-PM-7(1): Enterprise Architecture   Offloading</i>	25
P-PM-8: Critical Infrastructure Plan (CIP)	25
P-PM-9: Risk Management Strategy	26
P-PM-10: Authorization Process	27
P-PM-11: Mission & Business Process Definition	28
P-PM-12: Insider Threat Program	29
P-PM-13: Security & Privacy Workforce	30
P-PM-14: Testing, Training & Monitoring	30
P-PM-15: Security & Privacy Groups & Associations	31
P-PM-16: Threat Awareness Program	32
<i>P-PM-16(1): Threat Awareness Program   Automated Means for Sharing Threat Intelligence</i>	33
P-PM-17: Protecting CUI on External Systems	33
P-PM-18: Privacy Program Plan	34
P-PM-19: Privacy Program Leadership Role	35
P-PM-20: Dissemination of Privacy Program Information	36
<i>P-PM-20(1): Dissemination of Privacy Program Information   Privacy policies On Websites, Applications &amp; digital Services</i>	37
P-PM-21: Accounting of Disclosures	37
P-PM-22: Personally Identifiable Information (PII) Quality Management	38
P-PM-23: Data Governance Body	39
P-PM-24: Data Integrity Board	40
P-PM-25: Minimization of PII Used in Testing, Training & Research	41
P-PM-26: Complaint Management	41
P-PM-27: Privacy Reporting	42
P-PM-28: Risk Framing	43
P-PM-29: Risk Management Program Leadership Roles	44
P-PM-30: Supply Chain Risk Management Strategy	45
<i>P-PM-30(1): Supply Chain Risk Management Strategy   Suppliers or Critical or Mission-Essential items</i>	46
P-PM-31: Continuous Monitoring Strategy	46

P-PM-32: Purposing	47
<b>ASSESSMENT, AUTHORIZATION &amp; MONITORING (CA)</b>	<b>49</b>
P-CA-1: Assessment, Authorization & Monitoring Policy & Procedures	49
P-CA-2: Control Assessments	50
<i>P-CA-2(1): Control Assessments   Independent Assessors</i>	51
<i>P-CA-2(2): Control Assessments   Specialized Assessments</i>	52
<i>P-CA-2(3): Control Assessments   Leveraging Results from External Organizations</i>	53
P-CA-3: Information Exchange	53
P-CA-5: Plan of Action & Milestones (POA&M)	54
P-CA-6: Authorization	55
P-CA-7: Continuous Monitoring	56
<i>P-CA-7(1): Continuous Monitoring   Independent Assessment</i>	57
<i>P-CA-7(4): Continuous Monitoring   Risk Monitoring</i>	58
P-CA-8: Penetration Testing	60
<i>P-CA-8(1): Penetration Testing   Independent Penetration Agent or Team</i>	61
P-CA-9: Internal System Connections	61
<b>PLANNING (PL)</b>	<b>63</b>
P-PL-1: Planning Policy & Procedures	63
P-PL-2: System Security and Privacy Plans (SSPPs)	64
P-PL-4: Rules of Behavior	65
<i>P-PL-4(1): Rules Of Behavior   Social Media &amp; External Site / Application Usage Restrictions</i>	66
P-PL-8: Security& Privacy Architecture	67
P-PL-9: Central Management	68
P-PL-10: Baseline Selection	69
P-PL-11: Baseline Tailoring	70
<b>RISK ASSESSMENT (RA)</b>	<b>72</b>
P-RA-1: Risk Assessment Policy & Procedures	72
P-RA-2: Security Categorization	73
P-RA-3: Risk Assessment	74
<i>P-RA-3(1): Risk Assessment   Supply Chain Risk Assessment</i>	75
P-RA-5: Vulnerability Monitoring & Scanning	76
<i>P-RA-5(2): Vulnerability Monitoring &amp; Scanning   Update Vulnerabilities To Be Scanned</i>	77
<i>P-RA-5(3): Vulnerability Monitoring &amp; Scanning   Breadth &amp; Depth of Coverage</i>	78
<i>P-RA-5(5): Vulnerability Monitoring &amp; Scanning   Privileged Access</i>	79
<i>P-RA-5(6): Vulnerability Monitoring &amp; Scanning   Automated Trend Analysis</i>	79
<i>P-RA-5(8): Vulnerability Monitoring &amp; Scanning   Review Historical Audit Logs</i>	80
<i>P-RA-5(11): Vulnerability Monitoring &amp; Scanning   Public Disclosure Program</i>	81
P-RA-6: Technical Surveillance Countermeasures Security	81
P-RA-7: Risk Response	82
P-RA-8: Privacy Impact Assessments (PIA)	83
P-RA-9: Criticality Analysis	84
<b>SYSTEM &amp; SERVICE ACQUISITION (SA)</b>	<b>85</b>
P-SA-1: System & Services Acquisition Policy & Procedures	85
P-SA-2: Allocation of Resources	86
P-SA-3: System Development Life Cycle (SDLC)	86
P-SA-4: Acquisition Process	87
<i>P-SA-4(1): Acquisition Process   Functional Properties Of Controls</i>	88
<i>P-SA-4(2): Acquisition Process   Design &amp; Implementation of Controls</i>	89
<i>P-SA-4(8): Acquisition Process   Continuous Monitoring Plan for Controls</i>	90
<i>P-SA-4(9): Acquisition Process   Functions, Ports, Protocols &amp; Services In Use</i>	91
<i>P-SA-4(10): Acquisition Process   Use of Approved PIV Products</i>	91
P-SA-5: System Documentation	92
P-SA-8: Security & Privacy Engineering Principles	93
<i>P-SA-8(33): Security &amp; Privacy Engineering Principles   Minimization</i>	94
P-SA-9: External System Services	95
<i>P-SA-9(1): External System Services   Risk Assessments &amp; Organizational Approvals</i>	96

P-SA-9(2): External System Services   Identification Of Functions, Ports, Protocols & Services	97
P-SA-9(4): External System Services   Consistent Interests of Consumers & Providers	97
P-SA-9(5): External System Services   Processing, Storage & Service Location	98
P-SA-10: Developer Configuration Management	99
P-SA-10(1): Developer Configuration Management   Software & Firmware Integrity Verification	100
P-SA-11: Developer Testing & Evaluation	100
P-SA-11(1): Developer Testing & Evaluation   Static Code Analysis	101
P-SA-11(2): Developer Testing & Evaluation   Threat Modeling & Vulnerability Analysis	102
P-SA-11(8): Developer Testing & Evaluation   Dynamic Code Analysis	103
P-SA-15: Development Process, Standards & Tools	104
P-SA-15(3): Development Process, Standards & Tools   Criticality Analysis	105
P-SA-20: Customized Development of Critical Components	106
P-SA-22: Unsupported System Components	106
<b>SUPPLY CHAIN RISK MANAGEMENT (SR)</b>	<b>108</b>
P-SR-1: Supply Chain Risk Management Policy & Procedures	108
P-SR-2: Supply Chain Risk Management Plan	108
P-SR-2(1): Supply Chain Risk Management Plan   Establish SCRM Team	109
P-SR-3: Supply Chain Controls & Processes	110
P-SR-5: Acquisition Strategies, Tools & Methods	111
P-SR-6: Supplier Assessments & Reviews	112
P-SR-8: Notification Agreements	113
P-SR-10: Inspection of Systems or Components	114
P-SR-11: Component Authenticity	115
P-SR-11(1): Component Authenticity   Anti-Counterfeit Training	115
P-SR-11(2): Component Authenticity   Configuration Control for Component Service & Repair	116
P-SR-11(3): Component Authenticity   Anti-Counterfeit Scanning	117
P-SR-12: Component Disposal	118
<b>OPERATIONAL CONTROLS</b>	<b>119</b>
<b>AWARENESS &amp; TRAINING (AT)</b>	<b>119</b>
P-AT-1: Security Awareness & Training Policy & Procedures	119
P-AT-2: Literacy Awareness Training	120
P-AT-2(2): Literacy Awareness Training   Insider Threat	121
P-AT-2(3): Literacy Awareness Training   Social Engineering & Mining	122
P-AT-2(5): Literacy Awareness Training   Advanced Persistent Threat	122
P-AT-3: Role-Based Training	123
P-AT-3(5): Roles-Based Training   Processing PII	124
P-AT-4: Training Records	125
<b>CONTINGENCY PLANNING (CP)</b>	<b>126</b>
P-CP-1: Contingency Planning Policy & Procedures	126
P-CP-2: Contingency Plan	127
P-CP-2(1): Contingency Plan   Coordinate with Related Plans	128
P-CP-2(2): Contingency Plan   Capacity Planning	128
P-CP-2(3): Contingency Plan   Resume Mission & Business Functions	129
P-CP-2(8): Contingency Plan   Identify Critical Assets	130
P-CP-3: Contingency Training	130
P-CP-4: Contingency Plan Testing	131
P-CP-4(1): Contingency Plan Testing   Coordinate with Related Plans	132
P-CP-6: Alternate Storage Site	132
P-CP-6(1): Alternate Storage Site   Separation from Primary Site	133
P-CP-6(3): Alternate Storage Site   Accessibility	134
P-CP-7: Alternate Processing Site	135
P-CP-7(1): Alternate Processing Site   Separation from Primary Site	135
P-CP-7(2): Alternate Processing Site   Accessibility	136
P-CP-7(3): Alternate Processing Site   Priority of Service	137
P-CP-8: Telecommunications Services	137
P-CP-8(1): Telecommunications Services   Priority of Service Provisions	138

<i>P-CP-8(2): Telecommunications Services   Single Points of Failure</i>	139
P-CP-9: System Backup	140
<i>P-CP-9(1): System Backup   Testing for Reliability &amp; Integrity</i>	141
<i>P-CP-9(3): System Backup   Separate Storage for Critical Information</i>	141
<i>P-CP-9(5): System Backup   Transfer to Alternate Storage Site</i>	142
<i>P-CP-9(8): System Backup   Cryptographic Protection</i>	143
P-CP-10: System Recovery & Reconstitution	143
<i>P-CP-10(2): System Recovery &amp; Reconstitution   Transaction Recovery</i>	144
<b>INCIDENT RESPONSE (IR)</b>	<b>145</b>
P-IR-1: Incident Response Policy & Procedures	145
P-IR-2: Incident Response Training	146
<i>P-IR-2(3): Incident Response Training   Breach</i>	146
P-IR-3: Incident Response Testing	147
<i>P-IR-3(2): Incident Response Testing   Coordination with Related Plans</i>	148
P-IR-4: Incident Handling	148
<i>P-IR-4(1): Incident Handling   Automated Incident Handling Processes</i>	149
<i>P-IR-4(4): Incident Handling   Information Correlation</i>	150
<i>P-IR-4(5): Incident Handling   Automatic Disabling of System</i>	151
P-IR-5: Incident Monitoring	151
P-IR-6: Incident Reporting	152
<i>P-IR-6(1): Incident Reporting   Automated Reporting</i>	153
<i>P-IR-6(3): Incident Reporting   Supply Chain Coordination</i>	154
P-IR-7: Incident Reporting Assistance	154
<i>P-IR-7(1): Incident Reporting Assistance   Automation Support of Availability of Information &amp; Support</i>	155
<i>P-IR-7(2): Incident Reporting Assistance   Coordination With External Providers</i>	156
P-IR-8: Incident Response Plan (IRP)	156
<i>P-IR-8(1): Incident Response Plan (IRP)   Breaches</i>	158
P-IR-9: Information Spillage Response	159
<i>P-IR-9(2): Information Spillage Response   Training</i>	160
<i>P-IR-9(3): Information Spillage Response   Post-Spill Operations</i>	160
<i>P-IR-9(4): Information Spillage Response   Exposure to Unauthorized Personnel</i>	161
<b>MEDIA PROTECTION (MP)</b>	<b>163</b>
P-MP-1: Media Protection Policy & Procedures	163
P-MP-2: Media Access	164
P-MP-3: Media Marking	165
P-MP-4: Media Storage	165
P-MP-5: Media Transport	166
P-MP-6: Media Sanitization	167
<i>P-MP-6(2): Media Sanitization   Equipment Testing</i>	168
P-MP-7: Media Use	168
<b>PERSONNEL SECURITY (PS)</b>	<b>170</b>
P-PS-1: Personnel Security Policy & Procedures	170
P-PS-2: Position Risk Designation	171
P-PS-3: Personnel Screening	171
<i>P-PS-3(3): Personnel Screening   Information With Special Protection Measures</i>	172
P-PS-4: Personnel Termination	173
P-PS-5: Personnel Transfer	174
P-PS-6: Access Agreements	175
P-PS-7: External Personnel Security	176
P-PS-8: Personnel Sanctions	176
P-PS-9: Position Descriptions	177
<b>PHYSICAL &amp; ENVIRONMENTAL PROTECTION (PE)</b>	<b>179</b>
P-PE-1: Physical & Environmental Protection Policy & Procedures	179
P-PE-2: Physical Access Authorizations	180
P-PE-3: Physical Access Control	180
P-PE-4: Access Control For Transmission	182

P-PE-5: Access Control For Output Devices	182
P-PE-6: Monitoring Physical Access	183
<i>P-PE-6(1): Monitoring Physical Access   Intrusion Alarms &amp; Surveillance Equipment</i>	184
P-PE-8: Visitor Access Records	185
<i>P-PE-8(3): Visitor Access Records   Limit Personally Identifiable Information Elements</i>	186
P-PE-9: Power Equipment & Cabling	186
P-PE-10: Emergency Shutoff	187
P-PE-11: Emergency Power	188
P-PE-12: Emergency Lighting	188
P-PE-13: Fire Protection	189
<i>P-PE-13(1): Fire Protection   Detection Devices – Automatic Activation &amp; Notification</i>	190
<i>P-PE-13(2): Fire Protection   Suppression Systems – Automatic Activation &amp; Notification</i>	190
P-PE-14: Environmental Controls	191
<i>P-PE-14(2): Environmental Controls   Monitoring with Alarms &amp; Notifications</i>	192
P-PE-15: Water Damage Protection	192
P-PE-16: Delivery & Removal	193
P-PE-17: Alternate Work Site	194
P-PE-18: Location of Information System Components	195
P-PE-20: Asset Monitoring & Tracking	195
<b>PERSONALLY IDENTIFIABLE INFORMATION (PII) PROCESSING &amp; TRANSPARENCY</b>	<b>197</b>
P-PT-1: Policy and Procedures	197
P-PT-2: Authority to Process PII	198
P-PT-3: PII Processing Purposes	198
P-PT-4: Consent	199
P-PT-5: Privacy Notice	200
<i>P-PT-5(2): Privacy Notice   Privacy Act Statements</i>	201
P-PT-6: System of Records Notice (SORN)	201
<i>P-PT-6(1): System of Records Notice (SORN)   Routine Uses</i>	202
<i>P-PT-6(2): System of Records Notice (SORN)   Exemption Rules</i>	203
P-PT-7: Specific Categories of PII	203
<i>P-PT-7(1): Specific Categories of PII   Social Security Numbers (SSN)</i>	204
<i>P-PT-7(2): Specific Categories of PII   First Amendment Information</i>	205
P-PT-8: Computer Matching Requirements	205
<b>TECHNICAL CONTROLS</b>	<b>207</b>
<b>ACCESS CONTROL (AC)</b>	<b>207</b>
P-AC-1: Access Control Policy & Procedures	207
P-AC-2: Account Management	208
<i>P-AC-2(1): Account Management   Automated System Account Management</i>	209
<i>P-AC-2(2): Account Management   Removal of Temporary / Emergency Accounts</i>	210
<i>P-AC-2(3): Account Management   Disable Inactive Accounts</i>	211
<i>P-AC-2(4): Account Management   Automated Audit Actions</i>	211
<i>P-AC-2(5): Account Management   Inactivity Logout</i>	212
<i>P-AC-2(7): Account Management   Privileged User Accounts</i>	213
<i>P-AC-2(9): Account Management   Restrictions on Use of Shared Groups &amp; Accounts</i>	213
<i>P-AC-2(12): Account Management   Account Monitoring for Atypical Usage</i>	214
<i>P-AC-2(13): Account Management   Disable Accounts for High-Risk Individuals</i>	215
P-AC-3: Access Enforcement	215
<i>P-AC-3(14): Access Enforcement   Individual Access</i>	216
P-AC-4: Information Flow Enforcement	217
<i>P-AC-4(8): Information Flow Enforcement   Security &amp; Privacy Policy Filters</i>	218
<i>P-AC-4(21): Information Flow Enforcement   Physical or Logical Separation for Information Flows</i>	219
P-AC-5: Separation of Duties	220
P-AC-6: Least Privilege	221
<i>P-AC-6(1): Least Privilege   Authorize Access to Security Functions</i>	222
<i>P-AC-6(2): Least Privilege   Non-Privileged Access for Non-Security Functions</i>	223
<i>P-AC-6(5): Least Privilege   Privileged Accounts</i>	223
<i>P-AC-6(7): Least Privilege   Review of User Privileges</i>	224

<i>P-AC-6(9): Least Privilege   Auditing Use of Privileged Functions</i>	225
<i>P-AC-6(10): Least Privilege   Prohibit Non-Privileged Users from Executing Privileged Functions</i>	226
P-AC-7: Unsuccessful Logon Attempts	226
P-AC-8: System Use Notification (Logon Banner)	227
P-AC-10: Concurrent Session Control	229
P-AC-11: Device Lock	229
<i>P-AC-11(1): Device Lock   Pattern-Hiding Displays</i>	230
P-AC-12: Session Termination	231
P-AC-14: Permitted Actions Without Identification or Authorization	231
P-AC-17: Remote Access	232
<i>P-AC-17(1): Remote Access   Monitoring &amp; Control</i>	233
<i>P-AC-17(2): Remote Access   Protection of Confidentiality &amp; Integrity Using Encryption</i>	234
<i>P-AC-17(3): Remote Access   Managed Access Control Points</i>	234
<i>P-AC-17(4): Remote Access   Privileged Commands &amp; Access</i>	235
<i>P-AC-17(9): Remote Access   Disconnect or Disable Remote Access</i>	236
P-AC-18: Wireless Access	236
<i>P-AC-18(1): Wireless Access   Authentication &amp; Encryption</i>	237
<i>P-AC-18(3): Wireless Access   Disable Wireless Networking</i>	238
P-AC-19: Access Control For Mobile Devices	239
<i>P-AC-19(5): Access Control For Mobile Devices   Full Device or Container-Based Encryption</i>	240
P-AC-20: Use of External Systems	241
<i>P-AC-20(1): Use of External Systems   Limits of Authorized Use</i>	241
<i>P-AC-20(2): Use of External Systems   Portable Storage Devices – Restricted Use</i>	242
P-AC-21: Information Sharing	243
P-AC-22: Publicly Accessible Content	244
<b>AUDIT &amp; ACCOUNTABILITY (AU)</b>	<b>246</b>
P-AU-1: Audit & Accountability Policy & Procedures	246
P-AU-2: Event Logging	247
P-AU-3: Content of Audit Records	249
<i>P-AU-3(1): Content Of Audit Records   Additional Audit Information</i>	249
<i>P-AU-3(3): Content Of Audit Records   Limit Personally Identifiable Information Elements</i>	250
P-AU-4: Audit Log Storage Capacity	251
P-AU-5: Response To Audit Processing Failures	251
P-AU-6: Audit Review, Analysis & Reporting	252
<i>P-AU-6(1): Audit Review, Analysis &amp; Reporting   Automated Process Integration</i>	253
<i>P-AU-6(3): Audit Review, Analysis &amp; Reporting   Correlate Audit Record Repositories</i>	254
<i>P-AU-6(4): Audit Review, Analysis &amp; Reporting   Central Review &amp; Analysis</i>	255
P-AU-7: Audit Reduction & Report Generation	255
<i>P-AU-7(1): Audit Reduction &amp; Report Generation   Automatic Processing</i>	256
P-AU-8: Time Stamps	257
P-AU-9: Protection of Audit Information	257
<i>P-AU-9(2): Protection of Audit Information   Store on Separate Physical Systems or Components</i>	258
<i>P-AU-9(4): Protection of Audit Information   Access by Subset of Privileged Users</i>	259
P-AU-11: Audit Record Retention	259
P-AU-12: Audit Record Generation	260
P-AU-13: Monitoring For Information Disclosure	261
<b>CONFIGURATION MANAGEMENT (CM)</b>	<b>263</b>
P-CM-1: Configuration Management Policy & Procedures	263
P-CM-2: Baseline Configurations	264
<i>P-CM-2(2): Baseline Configuration   Automation Support for Accuracy &amp; Currency</i>	266
<i>P-CM-2(3): Baseline Configuration   Retention Of Previous Configurations</i>	267
<i>P-CM-2(7): Baseline Configuration   Configure Systems &amp; Components for High-Risk Areas</i>	267
P-CM-3: Configuration Change Control	268
<i>P-CM-3(2): Configuration Change Control   Testing, Validation &amp; Documentation of Changes</i>	269
<i>P-CM-3(4): Configuration Change Control   Security &amp; Privacy Representatives</i>	270
P-CM-4: Impact Analysis	270
<i>P-CM-4(2): Impact Analysis   Verification of Controls</i>	271

P-CM-5: Access Restrictions For Change	272
<i>P-CM-5(1): Access Restrictions For Change   Automated Access Enforcement &amp; Audit Records</i>	273
<i>P-CM-5(5): Access Restrictions For Change   Privilege Limitation for Production &amp; Operation (Incompatible Roles)</i>	273
P-CM-6: Configuration Settings	274
<i>P-CM-6(1): Configuration Settings   Automated Management, Application &amp; Verification</i>	276
P-CM-7: Least Functionality	276
<i>P-CM-7(1): Least Functionality   Periodic Review</i>	278
<i>P-CM-7(2): Least Functionality   Prevent Program Execution</i>	278
<i>P-CM-7(4): Least Functionality   Unauthorized Software (Blacklisting)</i>	279
<i>P-CM-7(5): Least Functionality   Authorized Software (Whitelisting)</i>	280
P-CM-8: System Component Inventory	280
<i>P-CM-8(1): System Component Inventory   Updates During Installation &amp; Removal</i>	281
<i>P-CM-8(3): System Component Inventory   Automated Unauthorized Component Detection</i>	282
P-CM-9: Configuration Management Plan	283
P-CM-10: Software Usage Restrictions	283
<i>P-CM-10(1): Software Usage Restrictions   Open Source Software</i>	284
P-CM-11: User-Installed Software	285
P-CM-12: Information Location	285
<i>P-CM-12(1): Information Location   Automated Tools To Support Information Location</i>	286
<b>IDENTIFICATION &amp; AUTHENTICATION (IA)</b>	<b>288</b>
P-IA-1: Identification & Authentication Policy & Procedures	288
P-IA-2: Identification & Authentication (Organizational Users)	289
<i>P-IA-2(1): Identification &amp; Authentication (Organizational Users)   Multi-Factor Authentication (MFA) to Privileged Accounts</i>	290
<i>P-IA-2(2): Identification &amp; Authentication (Organizational Users)   Multi-Factor Authentication (MFA) to Non-Privileged Accounts</i>	291
<i>P-IA-2(5): Identification &amp; Authentication (Organizational Users)   Individual Authentication With Group Authentication</i>	291
<i>P-IA-2(8): Identification &amp; Authentication (Organizational Users)   Access To Accounts - Replay Resistant</i>	292
<i>P-IA-2(12): Identification &amp; Authentication (Organizational Users)   Acceptance of PIV Credentials</i>	293
P-IA-3: Device Identification & Authentication	293
P-IA-4: Identifier Management (User Names)	294
<i>P-IA-4(4): Identifier Management   Identity User Status</i>	295
P-IA-5: Authenticator Management (Passwords)	296
<i>P-IA-5(1): Authenticator Management   Password-Based Authentication</i>	297
<i>P-IA-5(2): Authenticator Management   Public Key-Based Authentication</i>	299
<i>P-IA-5(6): Authenticator Management   Protection of Authenticators</i>	300
<i>P-IA-5(7): Authenticator Management   No Embedded Unencrypted Static Authenticators</i>	300
P-IA-6: Authenticator Feedback	301
P-IA-7: Cryptographic Module Authentication	302
P-IA-8: Identification & Authentication (Non-Organizational Users)	302
<i>P-IA-8(1): Identification &amp; Authentication (Non-Organizational Users)   Acceptance of PIV Credentials from Other Organizations</i>	303
<i>P-IA-8(2): Identification &amp; Authentication (Non-Organizational Users)   Acceptance of External Authenticators</i>	304
<i>P-IA-8(4): Identification &amp; Authentication (Non-Organizational Users)   Use of Defined Profiles</i>	304
P-IA-10: Adaptive Authentication	305
P-IA-11: Re-Authentication	306
P-IA-12: Identity Proofing	306
<i>P-IA-12(2): Identity Proofing   Identity Evidence</i>	307
<i>P-IA-12(3): Identity Proofing   Identity Evidence Validation &amp; Verification</i>	308
<i>P-IA-12(5): Identity Proofing   Address Confirmation</i>	308
<b>MAINTENANCE (MA)</b>	<b>310</b>
P-MA-1: Maintenance Policy & Procedures	310
P-MA-2: Controlled Maintenance	310
P-MA-3: Maintenance Tools	312
<i>P-MA-3(1): Maintenance Tools   Inspect Tools</i>	312
<i>P-MA-3(2): Maintenance Tools   Inspect Media</i>	313
<i>P-MA-3(3): Maintenance Tools   Prevent Unauthorized Removal</i>	314



P-MA-4: Non-Local Maintenance	314
<i>P-MA-4(6): Non-Local Maintenance   Cryptographic Protection</i>	315
P-MA-5: Maintenance Personnel	316
<i>P-MA-5(1): Maintenance Personnel   Individuals Without Appropriate Access</i>	316
P-MA-6: Timely Maintenance	317
<b>SYSTEM &amp; COMMUNICATION PROTECTION (SC)</b>	<b>319</b>
P-SC-1: System & Communication Policy & Procedures	319
P-SC-2: Separation of System & User Functionality	320
P-SC-4: Information In Shared Resources	320
P-SC-5: Denial of Service (DoS) Protection	321
P-SC-6: Resource Availability	322
P-SC-7: Boundary Protection	322
<i>P-SC-7(3): Boundary Protection   Access Points</i>	324
<i>P-SC-7(4): Boundary Protection   External Telecommunications Services</i>	324
<i>P-SC-7(5): Boundary Protection   Deny by Default - Allow by Exception (Access Control List)</i>	325
<i>P-SC-7(7): Boundary Protection   Split Tunneling for Remote Devices</i>	326
<i>P-SC-7(8): Boundary Protection   Route Traffic To Authenticated Proxy Servers</i>	326
<i>P-SC-7(12): Boundary Protection   Host-Based Protection</i>	327
<i>P-SC-7(13): Boundary Protection   Isolation of Security Tools, Mechanisms &amp; Support Components (Security Subnet)</i>	328
<i>P-SC-7(18): Boundary Protection   Fail Secure</i>	329
<i>P-SC-7(24): Boundary Protection   Personally Identifiable Information</i>	330
P-SC-8: Transmission Confidentiality & Integrity	331
<i>P-SC-8(1): Transmission Confidentiality &amp; Integrity   Cryptographic or Alternate Physical Protection</i>	332
P-SC-10: Network Disconnect	332
P-SC-12: Cryptographic Key Establishment & Management	333
<i>P-SC-12(2): Cryptographic Key Establishment &amp; Management   Symmetric Keys</i>	334
<i>P-SC-12(3): Cryptographic Key Establishment &amp; Management   Asymmetric Keys</i>	334
P-SC-13: Cryptographic Protection	335
P-SC-15: Collaborative Computing Devices & Applications	336
P-SC-17: Public Key Infrastructure (PKI) Certificates	337
P-SC-18: Mobile Code	337
P-SC-20: Secure Name / Address Resolution Service (Authoritative Source)	338
P-SC-21: Secure Name / Address Resolution Service (Recursive or Caching Resolver)	339
P-SC-22: Architecture & Provisioning For Name / Address Resolution Service	340
P-SC-23: Session Authenticity	341
P-SC-28: Protection of Information At Rest	341
<i>P-SC-28(1): Protection of Information at Rest   Cryptographic Protection</i>	342
P-SC-39: Process Isolation	343
P-SC-44: Detonation Chambers	344
P-SC-45: System Time Synchronization	345
<i>P-SC-45(1): System Time Synchronization   Synchronization With Authoritative Time Source</i>	345
<b>SYSTEM &amp; INFORMATION INTEGRITY (SI)</b>	<b>347</b>
P-SI-1: System & Information Integrity Policy & Procedures	347
P-SI-2: Flaw Remediation (Software Patching)	348
<i>P-SI-2(2): Flaw Remediation   Automated Flaw Remediation Status</i>	349
<i>P-SI-2(3): Flaw Remediation   Time To Remediate Flaws &amp; Benchmarks For Corrective Action</i>	350
P-SI-3: Malicious Code Protection (Malware)	350
P-SI-4: System Monitoring	352
<i>P-SI-4(1): System Monitoring   System-Wide Intrusion Detection System</i>	353
<i>P-SI-4(2): System Monitoring   Automated Tools for Real-Time Analysis</i>	353
<i>P-SI-4(4): System Monitoring   Inbound &amp; Outbound Communications Traffic</i>	354
<i>P-SI-4(5): System Monitoring   System Generated Alerts</i>	355
<i>P-SI-4(14): System Monitoring   Wireless Intrusion Detection</i>	355
<i>P-SI-4(16): System Monitoring   Correlate Monitoring Information</i>	356
<i>P-SI-4(23): System Monitoring   Host-Based Devices</i>	357
P-SI-5: Security Alerts, Advisories & Directives	357
P-SI-6: Security & Privacy Functionality Verification	358

P-SI-7: Software, Firmware & Information Integrity	359
<i>P-SI-7(1): Software, Firmware &amp; Information Integrity   Integrity Checks</i>	360
<i>P-SI-7(7): Software, Firmware &amp; Information Integrity   Integration of Detection &amp; Response</i>	361
P-SI-8: Spam Protection	361
<i>P-SI-8(2): Spam Protection   Automatic Updates</i>	362
P-SI-10: Input Data Validation	363
P-SI-11: Error Handling	363
P-SI-12: Information Output Handling & Retention	364
<i>P-SI-12(1): Information Management &amp; Retention   Limit Personally Identifiable Information Elements</i>	365
<i>P-SI-12(2): Information Management &amp; Retention   Minimize Personally Identifiable Information In Testing, Training &amp; Research</i>	366
<i>P-SI-12(3): Information Management &amp; Retention   Information Disposal</i>	366
P-SI-16: Memory Protection	367
P-SI-18: Personally Identifiable Information Quality Operations	367
<i>P-SI-18(4): Personally Identifiable Information Quality Operations   Individual Requests</i>	368
P-SI-19: De-Identification	368

---

**GLOSSARY: ACRONYMS & DEFINITIONS** **370**

**ACRONYMS** **370**

**DEFINITIONS** **370**

---

**RECORD OF CHANGES** **371**

EXAMPLE

## OVERVIEW, INSTRUCTIONS & EXAMPLE

### 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).

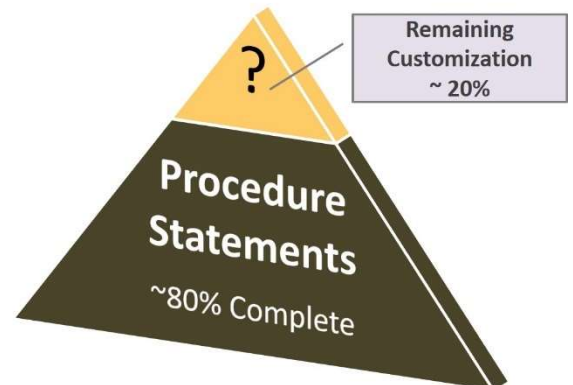
### OVERVIEW

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.

### UNDERSTANDING CONTROL OBJECTIVES & CONTROLS

As part of the CSOP, you will see Control Objectives and Controls for each of the CSOP procedures:

- The origin of the Control Objective is ComplianceForge’s [Cybersecurity & Data Protection Program \(CDPP\)](#) that consolidates multiple statutory, regulatory and contractual requirements into a single control objective.
- The origin of the Controls is the [Secure Controls Framework \(SCF\)](#) that is an open source set of cybersecurity and privacy controls.

Note - The footnotes at the bottom of the page and the accompanying Excel spreadsheet provide mapping between the control objectives, controls and leading frameworks, including statutory, regulatory and contractual obligations.

## 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.

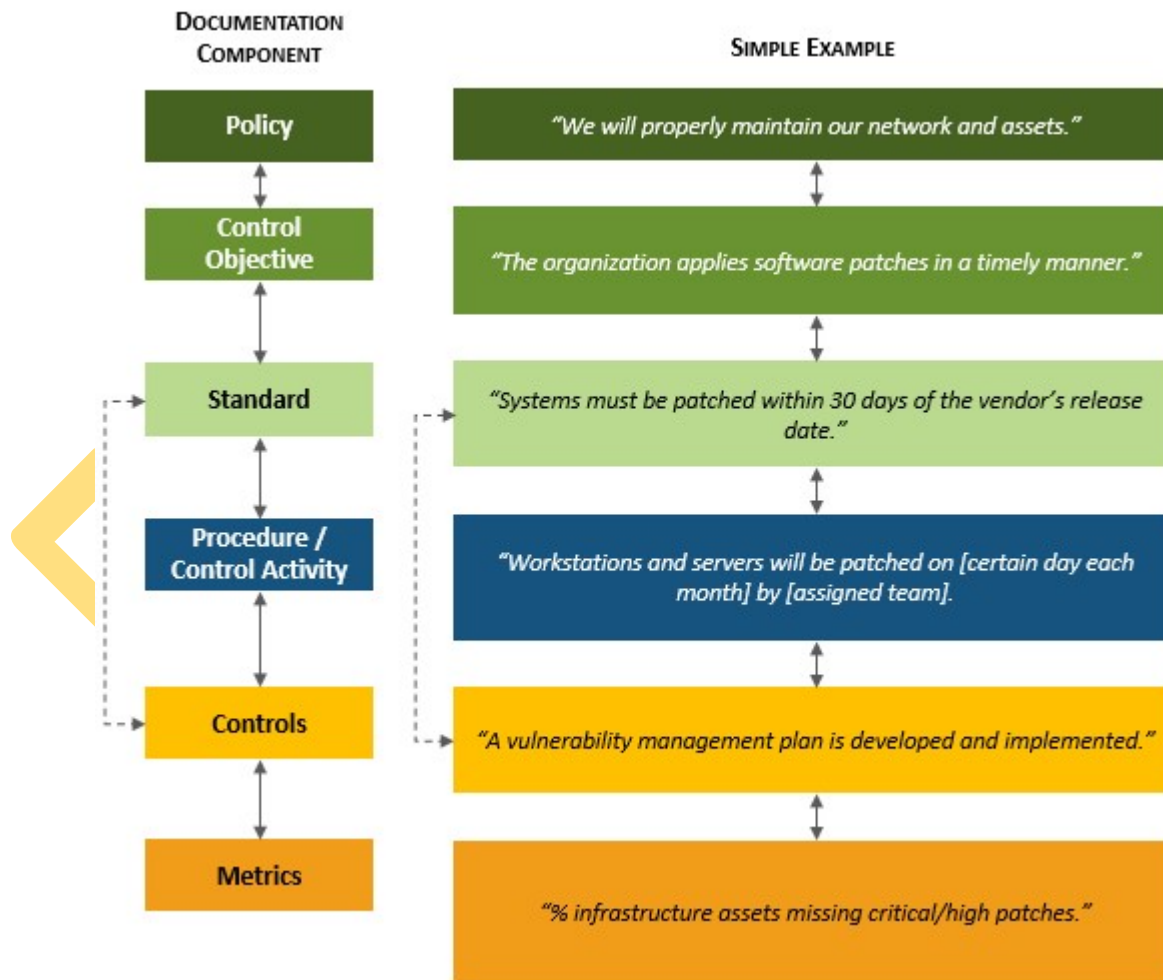
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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.<sup>1</sup> The purpose of this framework is that work roles have an impact on an organization's ability to protect its data, systems and operations. By assigning work roles, it helps direct the work of employees and contractors to minimize assumptions about who is responsible for certain cybersecurity and privacy tasks.

The CSOP uses the work roles identified in the NIST NICE Cybersecurity Workforce Framework to help make assigning the tasks associated with procedures/control activities more efficient and manageable. Keep in mind these are merely recommendations and are fully editable for every organization – this is just a helpful point in the right direction!



NIST NICE Cybersecurity Workforce Framework – Work Categories

### EXAMPLE PROCEDURE

This example is a configuration procedure **P-CM-2 (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*

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

Control Objective:<sup>2</sup>

- a. Develop, document and maintain under configuration control, a current baseline configuration of the system; and
- b. Review and update the baseline configuration of the system:
  1. Per organization-defined frequency;
  2. When required due to organization-defined circumstances; and
  3. When system components are installed or upgraded.

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 throughout the System Development Life Cycle (SDLC).<sup>3</sup>
- (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:<sup>4</sup>
  - 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

<sup>2</sup> NIST SP 800-53 Rev 5 control CM-2

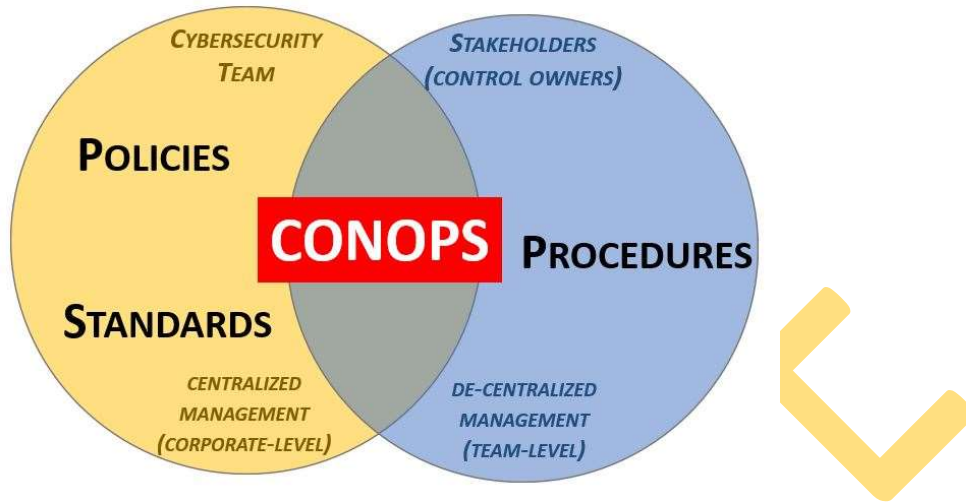
<sup>3</sup> NIST SP 800-171A assessment criteria 3.4.1[a] & 3.4.1[c]

<sup>4</sup> NIST SP 800-171A assessment criteria 3.4.1[b]

- 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 [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.
  - (8) If necessary, requests corrective action to address identified deficiencies.
  - (9) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
  - (10) If necessary, documents the results of corrective action and notes findings.
  - (11) If necessary, requests additional corrective action to address unremediated deficiencies.

**SUPPORTING POLICIES & STANDARDS**

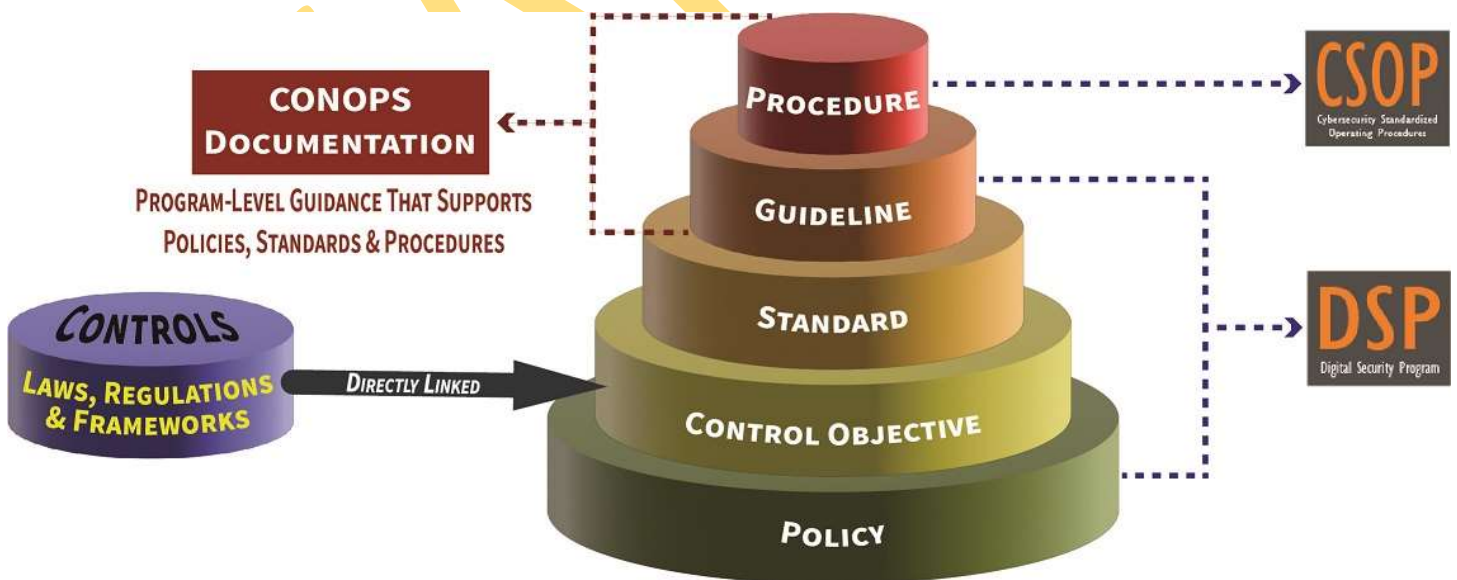
While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with ComplianceForge’s [NIST SP 800-53-based Cybersecurity & Data Protection Program \(CDPP\)](#) that contains policies, control objectives, standards and guidelines.



Concept of Operations (CONOPS) relationship.

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

As referenced in this graphic, a Concept of Operations (CONOPS) is a security-focused description that addresses life cycle concepts. This can include concepts for sustainment, logistics, maintenance and training. CONOPS augment and support an organization’s policies, standards and procedures. Examples of CONOPS documentation includes, but is not limited to:

- Risk management (e.g., Risk Management Program (RMP))
- Vulnerability management (e.g., Vulnerability & Patch Management Program (VPMP))



- Incident response (e.g., Integrated Incident Response Program (IIRP))
- Business Continuity / Disaster Recovery (e.g., Continuity of Operations Plan (COOP))
- Secure engineering practices (e.g., Security & Privacy By Design (SPBD))
- Pre-production testing (e.g., Information Assurance Program (IAP))
- Supply Chain Risk Management (SCRM) (e.g., Third-Party Security Management (TPSM))
- Configuration management (e.g., Secure Baseline Configurations (SBC))

EXAMPLE

---

## KNOWN COMPLIANCE REQUIREMENTS

---

ACME has certain compliance requirements that all team members need to be aware of:

### STATUTORY REQUIREMENTS

[fill-in applicable statutory requirements]

Example statutory requirements include:

- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Fair & Accurate Credit Transactions Act (FACTA)*
- *Sarbanes Ox ley Act (SOX)*
- *Gramm Leach Bliley Act (GLBA)*
- *Children's Online Privacy Protection Act (COPPA)*
- *Family Educational Rights and Privacy Act (FERPA)*
- *Massachusetts 201 CMR 17.00*
- *Oregon Identity Theft Protection Act (ORS 646A)*
- *United Kingdom Data Protection Act (UK DPA)*

### REGULATORY REQUIREMENTS

[fill-in applicable regulatory requirements]

Example regulatory requirements include:

- *Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012)*
- *NIST SP 800-171 / Cybersecurity Maturity Model Certification (CMMC)*
- *Federal Acquisition Regulation (FAR 52.204-21)*
- *European Union General Data Protection Regulation (EU GDPR)*
- *Financial Industry Regulatory Authority (FINRA)*
- *National Industrial Security Program Operating Manual (NISPOM)*
- *Department of Defense Information Assurance Risk Management Framework (DIARMF) (DoDI 8510.01)*
- *Federal Risk and Authorization Management Program (FedRAMP)*
- *New York Department of Financial Services (NY DFS) 23 NYCCRR 500*
- *North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)*

### CONTRACTUAL REQUIREMENTS

[fill-in applicable contractual requirements]

Example contractual requirements include:

- *ISO/IEC 27001 certification*
- *Payment Card Industry Data Security Standard (PCI DSS)*
- *Generally Accepted Privacy Principles (GAPP)*
- *American Institute of CPAs Service Organization Control (AICPA SOC2)*
- *Center for Internet Security Critical Security Controls (CIS CSC)*
- *Cloud Security Alliance Cloud Controls Matrix (CSA CCM)*

## MANAGEMENT CONTROLS

Management controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity topics. These cybersecurity controls address broader Information Security Management System (ISMS)-level governance of the security program that impact operational, technical and privacy controls.

### PROGRAM MANAGEMENT (PM)

#### P-PM-1: INFORMATION SECURITY PROGRAM PLAN

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:<sup>5</sup>

- a. Develop and disseminate an organization-wide information security program plan that:
  1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
  2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities and compliance;
  3. Reflects the coordination among organizational entities responsible for information security; and
  4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, other organizations and the Nation;
- b. Review and update the organization-wide information security program plan per an organization-defined frequency and following organization-defined events; and
- c. Protect the information security program plan from unauthorized disclosure and modification.

**Procedure / Control Activity:** Executive Cyber Leadership [OV-EXL-001], in conjunction with Privacy Officer/Privacy Compliance Manager [OV-LGA-002], Chief Risk Officer (CRO) [XX-RSK-001], Security Architect [SP-ARC-002] and Systems Security Manager [OV-MGT-001]:

- (1) Develops an organization-wide information security governance program to provide complete coverage for all cybersecurity and privacy-related controls needed to address statutory, regulatory and contractual obligations, as well as to address possible threats to data and or assets.
- (2) Documents the ACME information security program plan in a single document, the Cybersecurity & Data Protection Program (CDPP).
- (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.

<sup>5</sup> NIST SP 800-53 Rev 5 control PM-1

## ASSESSMENT, AUTHORIZATION & MONITORING (CA)

### P-CA-1: ASSESSMENT, AUTHORIZATION & MONITORING POLICY & PROCEDURES

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:<sup>46</sup>

- a. Develop, document and disseminate to organization-defined personnel or roles:
  1. Organization-level assessment, authorization and monitoring policy that:
    - (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and
    - (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards and guidelines; and
  2. Procedures to facilitate the implementation of the assessment, authorization and monitoring policy and the associated assessment, authorization and monitoring controls;
- b. Designate an organization-defined official to manage the development, documentation and dissemination of the assessment, authorization and monitoring policy and procedures; and
- c. Review and update the current assessment, authorization and monitoring:
  1. Policy per an organization-defined frequency and following organization-defined events; and
  2. Procedures per an organization-defined frequency and following organization-defined events.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001], in conjunction with Privacy Officer/Privacy Compliance Manager [OV-LGA-002], Chief Risk Officer (CRO) [XX-RSK-001], Security Architect [SP-ARC-002] and Systems Security Manager [OV-MGT-001]:

- (1) Develops an organization-wide secure engineer practices program that leverages ACME-adopted cybersecurity and privacy principles.
- (2) Documents an assessment, authorization & monitoring policy and standards in a single document, the Cybersecurity & Data Protection Program (CDPP).
- (3) Requires data/process owners and asset custodians to:
  - a. Document function-specific procedures in a Cybersecurity Standardized Operating Procedures (CSOP), or similar format;
  - b. Identify applicable statutory, regulatory and contractual obligations (see CDPP Applicability Matrix); and
  - c. Include the identification and assignment of roles and responsibilities among internal and external stakeholders.
- (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.

<sup>46</sup> NIST SP 800-53 Rev 5 control CA-1

## P-CA-2: CONTROL ASSESSMENTS

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:<sup>47</sup>

- a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;
- b. Develop a control assessment plan that describes the scope of the assessment including:
  1. Controls and control enhancements under assessment;
  2. Assessment procedures to be used to determine control effectiveness; and
  3. Assessment environment, assessment team and assessment roles and responsibilities;
- c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
- d. Assess the controls in the system and its environment of operation per an organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting established security and privacy requirements;
- e. Produce a control assessment report that document the results of the assessment; and
- f. Provide the results of the control assessment to organization-defined individuals or roles.

### Procedure / Control Activity: Governance Manager [XX-GRC-001], in coordination with Governance Specialist [XX-GRC-002]:

1. Uses industry-recognized secure practices to ensure controls are sufficient for conducting cybersecurity assessments that includes:
  - a. A formal, documented cybersecurity assessment program;
  - b. Processes to facilitate the implementation of cybersecurity assessments;
  - c. Processes to review systems in production, since production systems may deviate significantly from the functional and design specifications created during the requirements and design phases of the Secure Development Life Cycle (SDLC). Therefore, threat and vulnerability analysis needs to address new vulnerabilities created as a result of those changes have been reviewed and mitigated:
    - i. Addressing new threats and vulnerabilities on an ongoing basis and ensures these applications are protected against known attacks by either of the following methods:
      1. Reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any change; or
      2. Installing an application firewall.
    - ii. Verifying that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows:
      1. At least annually;
      2. After any changes;
      3. By an organization that specializes in application security;
      4. That all vulnerabilities are corrected; and
      5. That the application is re-evaluated after the corrections.
2. Implements appropriate physical, administrative and technical means to implement a Control Validation Testing (CVT) program to validate cybersecurity and privacy controls are:<sup>48</sup>
  - a. Implemented correctly;
  - b. Operating as intended; and

<sup>47</sup> NIST SP 800-53 Rev 5 control CA-2

<sup>48</sup> NIST SP 800-171A assessment criteria 3.12.1[b]

### **P-IR-3(2): INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS**

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:** Coordinate incident response testing with organizational elements responsible for related plans.<sup>207</sup>

**Procedure / Control Activity:** Systems Security Manager [OV-MGT-001], in conjunction with Asset Owner [XX-AST-001], Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

- (1) Implements appropriate administrative means to ensure identify key personnel associated with related plans (e.g., Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), etc.).
- (2) Coordinates incident response testing with appropriate personnel responsible for related plans.
- (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-IR-4: INCIDENT HANDLING**

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:**<sup>208</sup>

- a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication and recovery;
- b. Coordinate incident handling activities with contingency planning activities;

<sup>207</sup> NIST SP 800-53 Rev 5 control IR-3(2)

<sup>208</sup> NIST SP 800-53 Rev 5 control IR-4

- c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training and testing and implement the resulting changes accordingly; and
- d. Ensure the rigor, intensity, scope and results of incident handling activities are comparable and predictable across the organization.

**Procedure / Control Activity:** Cyber Defense Incident Responder [PR-CIR-001], in conjunction with Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

- (1) Leverages ACME's Integrated Incident Response Program (IIRP) to: <sup>209</sup>
  - a. Investigate notifications from detection systems;
  - b. Identify and assess the severity and classification of incidents;
  - c. Define appropriate user response activities to take in response to the incident, in accordance with ACME's Incident Response Plan (IRP); <sup>210</sup>
  - d. Respond with appropriate remediation actions to minimize impact and ensure the continuation of business functions; and
  - e. As necessary, update the IRP, based on lessons learned from the incident.
- (2) Ensures the IIRP includes:
  - a. Preparation; <sup>211</sup>
  - b. Detection; <sup>212</sup>
  - c. Analysis; <sup>213</sup>
  - d. Containment; <sup>214</sup> and
  - e. Recovery. <sup>215</sup>
- (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-IR-4(1): INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES**

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:** Support the incident handling process using automated mechanisms. <sup>216</sup>

**Procedure / Control Activity:** Cyber Defense Incident Responder [PR-CIR-001], in conjunction with Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

<sup>209</sup> NIST SP 800-171A assessment criteria 3.6.1[a]

<sup>210</sup> NIST SP 800-171A assessment criteria 3.6.1[g]

<sup>211</sup> NIST SP 800-171A assessment criteria 3.6.1[b]

<sup>212</sup> NIST SP 800-171A assessment criteria 3.6.1[c]

<sup>213</sup> NIST SP 800-171A assessment criteria 3.6.1[d]

<sup>214</sup> NIST SP 800-171A assessment criteria 3.6.1[e]

<sup>215</sup> NIST SP 800-171A assessment criteria 3.6.1[f]

<sup>216</sup> NIST SP 800-53 Rev 5 control IR-4(1)

- (1) Uses vendor-recommended settings and industry-recognized secure practices to employ automated mechanisms to support the incident handling process. Automated mechanisms supporting incident handling processes include, for example, online incident management systems.
- (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-IR-4(4): INCIDENT HANDLING | INFORMATION CORRELATION**

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:** Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.<sup>217</sup>

**Procedure / Control Activity:** Systems Security Manager [OV-MGT-001], in conjunction with Systems Security Analyst [OM-ANA-001], Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-02 and Cyber Defense Incident Responder [PR-CIR-001]:

- (1) Implements appropriate physical, administrative and technical means to implement automated mechanisms to integrate incident review, analysis and reporting processes to support organization-wide situational awareness for investigation and response to suspicious activities.
- (2) Maintains situational awareness through aggregating and correlating event data from multiple sources and sensors:
  - a. Helpdesk / service desk incidents;
  - b. Security Incident Event Manager (SIEM);
  - c. File Integrity Monitor (FIM);
  - d. Data Loss Prevention (DLP);
  - e. Intrusion Detection System / Intrusion Prevention System (IDS / IPS); and
  - f. Network Access Control (NAC).
- (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.

<sup>217</sup> NIST SP 800-53 Rev 5 control IR-4(4)



## **P-IR-4(5): INCIDENT HANDLING | AUTOMATIC DISABLING OF SYSTEM**

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:** Implement a configurable capability to automatically disable the system if organization-defined security violations are detected.<sup>218</sup>

**Procedure / Control Activity:** Security Architect [SP-ARC-002], in conjunction with Systems Security Manager [OV-MGT-001]:

- (1) Develops a list of ACME-defined security violations that upon detection would require automatic disabling of a system.
- (2) Uses vendor-recommended settings and industry-recognized secure practices to implement a configurable capability to automatically disable a system
- (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-IR-5: INCIDENT MONITORING**

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:** Track and document incidents.<sup>219</sup>

**Procedure / Control Activity:** Systems Security Manager [OV-MGT-001], in conjunction with Systems Security Analyst [OM-ANA-001], Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-02 and Cyber Defense Incident Responder [PR-CIR-001]:

<sup>218</sup> NIST SP 800-53 Rev 5 control IR-4(5)

<sup>219</sup> NIST SP 800-53 Rev 5 control IR-5

- (1) Implements appropriate physical, administrative and technical means to implement mechanisms to monitor for cybersecurity incidents.
- (2) Maintains situational awareness through aggregating and correlating event data from multiple sources and sensors:
  - a. Helpdesk / service desk incidents;
  - b. Security Incident Event Manager (SIEM);
  - c. File Integrity Monitor (FIM);
  - d. Data Loss Prevention (DLP);
  - e. Intrusion Detection System / Intrusion Prevention System (IDS / IPS); and
  - f. Network Access Control (NAC).
- (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-IR-6: INCIDENT REPORTING

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security & Privacy Plan (SSPP) 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:<sup>220</sup>

- a. Require personnel to report suspected incidents to the organizational incident response capability within an organization-defined time period; and
- b. Report incident information to organization-defined authorities.

**Procedure / Control Activity:** Systems Security Manager [OV-MGT-001], in conjunction with Cyber Defense Incident Responder [PR-CIR-001] and Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-002]:

- (1) Leverages ACME's Integrated Incident Response Program (IIRP) to:
  - a. Report actual or suspected cybersecurity incidents by:
    - i. Requiring users to report system weaknesses, deficiencies, and/or vulnerabilities through appropriate management channels as quickly as possible; and
    - ii. Involving management in suspected cybersecurity events quickly as possible.
  - b. Track incidents through resolution;<sup>221</sup>
  - c. Thoroughly document incidents;<sup>222</sup>
  - d. Identify the:
    - i. Statutory and/or regulatory authorities to whom incidents are to be reported, when applicable;<sup>223</sup> and
    - ii. ACME leadership personnel to whom incidents are to be reported;<sup>224</sup> and

<sup>220</sup> NIST SP 800-53 Rev 5 control IR-6

<sup>221</sup> NIST SP 800-171A assessment criteria 3.6.2[a]

<sup>222</sup> NIST SP 800-171A assessment criteria 3.6.2[b]

<sup>223</sup> NIST SP 800-171A assessment criteria 3.6.2[c]

<sup>224</sup> NIST SP 800-171A assessment criteria 3.6.2[d]