

YOUR LOGO GOES HERE

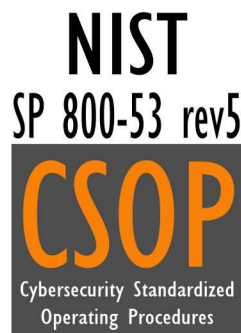
---

# CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

---

*[NIST SP 800 53 REV5 – LOW, MODERATE & HIGH 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>13</b>
<b>KEY TERMINOLOGY</b>	<b>13</b>
<b>OVERVIEW</b>	<b>13</b>
Customization Guidance	13
Validating Needs for Procedures / Control Activities	13
<b>UNDERSTANDING CONTROL OBJECTIVES &amp; CONTROLS</b>	<b>13</b>
<b>PROCEDURES DOCUMENTATION</b>	<b>14</b>
NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	15
Example Procedure	15
Supporting Policies & Standards	18
<b>KNOWN COMPLIANCE REQUIREMENTS</b>	<b>20</b>
<b>STATUTORY REQUIREMENTS</b>	<b>20</b>
<b>REGULATORY REQUIREMENTS</b>	<b>20</b>
<b>CONTRACTUAL REQUIREMENTS</b>	<b>20</b>
<b>MANAGEMENT CONTROLS</b>	<b>21</b>
<b>PROGRAM MANAGEMENT (PM)</b>	<b>21</b>
P-PM-1: Information Security Program Plan	21
P-PM-2: Information Security Program Leadership Role	22
P-PM-3: Information Security and Privacy Resources	22
P-PM-4: Plan of Action & Milestones (POA&M) Process (Vulnerability Remediation)	23
P-PM-5: System Inventory	24
<i>PM-5(1): System Inventory   Inventory of Personally Identifiable Information (PII)</i>	25
P-PM-6: Measures of Performance (Metrics)	25
P-PM-7: Enterprise Architecture	26
<i>P-PM-7(1): Enterprise Architecture   Offloading</i>	27
P-PM-8: Critical Infrastructure Plan (CIP)	27
P-PM-9: Risk Management Strategy	28
P-PM-10: Authorization Process	29
P-PM-11: Mission & Business Process Definition	30
P-PM-12: Insider Threat Program	31
P-PM-13: Security & Privacy Workforce	32
P-PM-14: Testing, Training & Monitoring	32
P-PM-15: Security & Privacy Groups & Associations	33
P-PM-16: Threat Awareness Program	34
<i>P-PM-16(1): Threat Awareness Program   Automated Means for Sharing Threat Intelligence</i>	35
P-PM-17: Protecting CUI on External Systems	35
P-PM-18: Privacy Program Plan	36
P-PM-19: Privacy Program Leadership Role	37
P-PM-20: Dissemination of Privacy Program Information	38
<i>P-PM-20(1): Dissemination of Privacy Program Information   Privacy policies On Websites, Applications &amp; Digital Services</i>	39
P-PM-21: Accounting of Disclosures	39
P-PM-22: Personally Identifiable Information (PII) Quality Management	40
P-PM-23: Data Governance Body	41
P-PM-24: Data Integrity Board	42
P-PM-25: Minimization of PII Used in Testing, Training & Research	43
P-PM-26: Complaint Management	43
P-PM-27: Privacy Reporting	44
P-PM-28: Risk Framing	45
P-PM-29: Risk Management Program Leadership Roles	46
P-PM-30: Supply Chain Risk Management Strategy	47
<i>P-PM-30(1): Supply Chain Risk Management Strategy   Suppliers or Critical or Mission-Essential items</i>	48
P-PM-31: Continuous Monitoring Strategy	48

P-PM-32: Purposing	49
<b>ASSESSMENT, AUTHORIZATION &amp; MONITORING (CA)</b>	<b>51</b>
P-CA-1: Assessment, Authorization & Monitoring Policy & Procedures	51
P-CA-2: Control Assessments	52
<i>P-CA-2(1): Control Assessments   Independent Assessors</i>	53
<i>P-CA-2(2): Control Assessments   Specialized Assessments</i>	54
<i>P-CA-2(3): Control Assessments   Leveraging Results from External Organizations</i>	55
P-CA-3: Information Exchange	55
<i>P-CA-3(6): Information Exchange   Transfer Authorizations</i>	56
P-CA-5: Plan of Action & Milestones (POA&M)	57
P-CA-6: Authorization	57
P-CA-7: Continuous Monitoring	58
<i>P-CA-7(1): Continuous Monitoring   Independent Assessment</i>	60
<i>P-CA-7(3): Continuous Monitoring   Trend Analysis</i>	61
<i>P-CA-7(4): Continuous Monitoring   Risk Monitoring</i>	61
P-CA-8: Penetration Testing	63
<i>P-CA-8(1): Penetration Testing   Independent Penetration Agent or Team</i>	64
<i>P-CA-8(2): Penetration Testing   Red Team Exercises</i>	65
P-CA-9: Internal System Connections	65
<b>PLANNING (PL)</b>	<b>67</b>
P-PL-1: Planning Policy & Procedures	67
P-PL-2: System Security and Privacy Plans (SSPPs)	68
P-PL-4: Rules of Behavior	69
<i>P-PL-4(1): Rules Of Behavior   Social Media &amp; External Site / Application Usage Restrictions</i>	70
P-PL-8: Security& Privacy Architecture	71
P-PL-9: Central Management	72
P-PL-10: Baseline Selection	73
P-PL-11: Baseline Tailoring	74
<b>RISK ASSESSMENT (RA)</b>	<b>76</b>
P-RA-1: Risk Assessment Policy & Procedures	76
P-RA-2: Security Categorization	77
P-RA-3: Risk Assessment	78
<i>P-RA-3(1): Risk Assessment   Supply Chain Risk Assessment</i>	79
<i>P-RA-3(3): Risk Assessment   Dynamic Threat Awareness</i>	80
<i>P-RA-3(4): Risk Assessment   Predictive Cyber Analytics</i>	80
P-RA-5: Vulnerability Monitoring & Scanning	81
<i>P-RA-5(2): Vulnerability Monitoring &amp; Scanning   Update Vulnerabilities To Be Scanned</i>	82
<i>P-RA-5(3): Vulnerability Monitoring &amp; Scanning   Breadth &amp; Depth of Coverage</i>	83
<i>P-RA-5(4): Vulnerability Monitoring &amp; Scanning   Discoverable Information</i>	84
<i>P-RA-5(5): Vulnerability Monitoring &amp; Scanning   Privileged Access</i>	84
<i>P-RA-5(6): Vulnerability Monitoring &amp; Scanning   Automated Trend Analysis</i>	85
<i>P-RA-5(8): Vulnerability Monitoring &amp; Scanning   Review Historical Audit Logs</i>	86
<i>P-RA-5(10): Vulnerability Monitoring &amp; Scanning   Correlate Scanning Information</i>	86
<i>P-RA-5(11): Vulnerability Monitoring &amp; Scanning   Public Disclosure Program</i>	87
P-RA-6: Technical Surveillance Countermeasures Security	88
P-RA-7: Risk Response	89
P-RA-8: Privacy Impact Assessments (PIA)	89
P-RA-9: Criticality Analysis	90
P-RA-10: Threat Hunting	91
<b>SYSTEM &amp; SERVICE ACQUISITION (SA)</b>	<b>93</b>
P-SA-1: System & Services Acquisition Policy & Procedures	93
P-SA-2: Allocation of Resources	94
P-SA-3: System Development Life Cycle (SDLC)	94
P-SA-4: Acquisition Process	95
<i>P-SA-4(1): Acquisition Process   Functional Properties Of Controls</i>	96
<i>P-SA-4(2): Acquisition Process   Design &amp; Implementation of Controls</i>	97

<i>P-SA-4(5): Acquisition Process   System, Component &amp; Service Configurations</i>	98
<i>P-SA-4(8): Acquisition Process   Continuous Monitoring Plan for Controls</i>	99
<i>P-SA-4(9): Acquisition Process   Functions, Ports, Protocols &amp; Services In Use</i>	99
<i>P-SA-4(10): Acquisition Process   Use of Approved PIV Products</i>	100
P-SA-5: System Documentation	100
P-SA-8: Security & Privacy Engineering Principles	102
<i>P-SA-8(33): Security &amp; Privacy Engineering Principles   Minimization</i>	103
P-SA-9: External System Services	103
<i>P-SA-9(1): External System Services   Risk Assessments &amp; Organizational Approvals</i>	104
<i>P-SA-9(2): External System Services   Identification Of Functions, Ports, Protocols &amp; Services</i>	105
<i>P-SA-9(4): External System Services   Consistent Interests of Consumers &amp; Providers</i>	106
<i>P-SA-9(5): External System Services   Processing, Storage &amp; Service Location</i>	106
P-SA-10: Developer Configuration Management	107
<i>P-SA-10(1): Developer Configuration Management   Software &amp; Firmware Integrity Verification</i>	108
P-SA-11: Developer Testing & Evaluation	109
<i>P-SA-11(1): Developer Testing &amp; Evaluation   Static Code Analysis</i>	110
<i>P-SA-11(2): Developer Testing &amp; Evaluation   Threat Modeling &amp; Vulnerability Analysis</i>	110
<i>P-SA-11(8): Developer Testing &amp; Evaluation   Dynamic Code Analysis</i>	111
P-SA-15: Development Process, Standards & Tools	112
<i>P-SA-15(3): Development Process, Standards &amp; Tools   Criticality Analysis</i>	113
P-SA-16: Developer-Provided Training	114
P-SA-17: Developer Security & Privacy Architecture & Design	115
<i>P-SA-17(9): Developer Security &amp; Privacy Architecture &amp; Design   Design Diversity</i>	116
P-SA-20: Customized Development of Critical Components	117
P-SA-21: Developer Screening	117
P-SA-22: Unsupported System Components	118
<b>SUPPLY CHAIN RISK MANAGEMENT (SR)</b>	<b>120</b>
P-SR-1: Supply Chain Risk Management Policy & Procedures	120
P-SR-2: Supply Chain Risk Management Plan	120
<i>P-SR-2(1): Supply Chain Risk Management Plan   Establish SCRM Team</i>	121
P-SR-3: Supply Chain Controls & Processes	122
P-SR-5: Acquisition Strategies, Tools & Methods	123
P-SR-6: Supplier Assessments & Reviews	124
<i>P-SR-6(1): Supplier Assessments &amp; Reviews   Testing &amp; Analysis</i>	125
P-SR-8: Notification Agreements	126
P-SR-9: Tamper Resistance & Detection	127
<i>P-SR-9(1): Tamper Resistance &amp; Detection   Multiple Stages of System Development Life Cycle (SDLC)</i>	127
P-SR-10: Inspection of Systems or Components	128
P-SR-11: Component Authenticity	129
<i>P-SR-11(1): Component Authenticity   Anti-Counterfeit Training</i>	130
<i>P-SR-11(2): Component Authenticity   Configuration Control for Component Service &amp; Repair</i>	130
<i>P-SR-11(3): Component Authenticity   Anti-Counterfeit Scanning</i>	131
P-SR-12: Component Disposal	132
<b>OPERATIONAL CONTROLS</b>	<b>133</b>
<b>AWARENESS &amp; TRAINING (AT)</b>	<b>133</b>
P-AT-1: Security Awareness & Training Policy & Procedures	133
P-AT-2: Literacy Awareness Training	134
<i>P-AT-2(1): Literacy Awareness Training   Practical Exercises</i>	135
<i>P-AT-2(2): Literacy Awareness Training   Insider Threat</i>	136
<i>P-AT-2(3): Literacy Awareness Training   Social Engineering &amp; Mining</i>	136
<i>P-AT-2(4): Literacy Awareness Training   Suspicious Communications &amp; Anomalous System Behavior</i>	137
<i>P-AT-2(5): Literacy Awareness Training   Advanced Persistent Threat</i>	138
<i>P-AT-2(6): Literacy Awareness Training   Cyber Threat Environment</i>	138
P-AT-3: Role-Based Training	139
<i>P-AT-3(3): Roles-Based Training   Practical Exercises</i>	140
<i>P-AT-3(5): Roles-Based Training   Processing PII</i>	141
P-AT-4: Training Records	142

<b>CONTINGENCY PLANNING (CP)</b>	<b>143</b>
P-CP-1: Contingency Planning Policy & Procedures	143
P-CP-2: Contingency Plan	144
<i>P-CP-2(1): Contingency Plan   Coordinate with Related Plans</i>	145
<i>P-CP-2(2): Contingency Plan   Capacity Planning</i>	145
<i>P-CP-2(3): Contingency Plan   Resume Mission &amp; Business Functions</i>	146
<i>P-CP-2(5): Contingency Plan   Continue Mission &amp; Business Functions</i>	147
<i>P-CP-2(8): Contingency Plan   Identify Critical Assets</i>	147
P-CP-3: Contingency Training	148
<i>P-CP-3(1): Contingency Training   Simulated Events</i>	149
P-CP-4: Contingency Plan Testing	149
<i>P-CP-4(1): Contingency Plan Testing   Coordinate with Related Plans</i>	150
<i>P-CP-4(2): Contingency Plan Testing   Alternate Processing Site</i>	151
P-CP-6: Alternate Storage Site	151
<i>P-CP-6(1): Alternate Storage Site   Separation from Primary Site</i>	152
<i>P-CP-6(2): Alternate Storage Site   Recovery Time &amp; Recovery Point Objectives</i>	153
<i>P-CP-6(3): Alternate Storage Site   Accessibility</i>	153
P-CP-7: Alternate Processing Site	154
<i>P-CP-7(1): Alternate Processing Site   Separation from Primary Site</i>	155
<i>P-CP-7(2): Alternate Processing Site   Accessibility</i>	156
<i>P-CP-7(3): Alternate Processing Site   Priority of Service</i>	156
<i>P-CP-7(4): Alternate Processing Site   Preparation for Use</i>	157
P-CP-8: Telecommunications Services	158
<i>P-CP-8(1): Telecommunications Services   Priority of Service Provisions</i>	159
<i>P-CP-8(2): Telecommunications Services   Single Points of Failure</i>	159
<i>P-CP-8(3): Telecommunications Services   Separation of Primary / Alternate Providers</i>	160
<i>P-CP-8(4): Telecommunications Services   Provider Contingency Plan</i>	161
P-CP-9: System Backup	161
<i>P-CP-9(1): System Backup   Testing for Reliability &amp; Integrity</i>	163
<i>P-CP-9(2): System Backup   Test Restoration Using Sampling</i>	163
<i>P-CP-9(3): System Backup   Separate Storage for Critical Information</i>	164
<i>P-CP-9(5): System Backup   Transfer to Alternate Storage Site</i>	164
<i>P-CP-9(7): System Backup   Dual Authorization</i>	165
<i>P-CP-9(8): System Backup   Cryptographic Protection</i>	166
P-CP-10: System Recovery & Reconstitution	166
<i>P-CP-10(2): System Recovery &amp; Reconstitution   Transaction Recovery</i>	167
<i>P-CP-10(4): System Recovery &amp; Reconstitution   Restore Within Time Period</i>	167
<b>INCIDENT RESPONSE (IR)</b>	<b>169</b>
P-IR-1: Incident Response Policy & Procedures	169
P-IR-2: Incident Response Training	170
<i>P-IR-2(1): Incident Response Training   Simulated Events</i>	170
<i>P-IR-2(2): Incident Response Training   Automated Training Environments</i>	171
<i>P-IR-2(3): Incident Response Training   Breach</i>	172
P-IR-3: Incident Response Testing	172
<i>P-IR-3(2): Incident Response Testing   Coordination with Related Plans</i>	173
P-IR-4: Incident Handling	173
<i>P-IR-4(1): Incident Handling   Automated Incident Handling Processes</i>	174
<i>P-IR-4(2): Incident Handling   Dynamic Reconfiguration</i>	175
<i>P-IR-4(3): Incident Handling   Continuity of Operations</i>	176
<i>P-IR-4(4): Incident Handling   Information Correlation</i>	177
<i>P-IR-4(5): Incident Handling   Automatic Disabling of System</i>	178
<i>P-IR-4(6): Incident Handling   Insider Threats</i>	179
<i>P-IR-4(8): Incident Handling   Correlation with External Organizations</i>	180
<i>P-IR-4(11): Incident Handling   Integrated Incident Response Team</i>	180
<i>P-IR-4(14): Incident Handling   Security Operations Center (SOC)</i>	181
P-IR-5: Incident Monitoring	182
<i>P-IR-5(1): Incident Monitoring   Automated Tracking, Data Collection &amp; Analysis</i>	183
P-IR-6: Incident Reporting	183



<i>P-IR-6(1): Incident Reporting   Automated Reporting</i>	185
<i>P-IR-6(3): Incident Reporting   Supply Chain Coordination</i>	185
P-IR-7: Incident Reporting Assistance	186
<i>P-IR-7(1): Incident Reporting Assistance   Automation Support of Availability of Information &amp; Support</i>	187
<i>P-IR-7(2): Incident Reporting Assistance   Coordination With External Providers</i>	187
P-IR-8: Incident Response Plan (IRP)	188
<i>P-IR-8(1): Incident Response Plan (IRP)   Breaches</i>	189
P-IR-9: Information Spillage Response	190
<i>P-IR-9(2): Information Spillage Response   Training</i>	191
<i>P-IR-9(3): Information Spillage Response   Post-Spill Operations</i>	192
<i>P-IR-9(4): Information Spillage Response   Exposure to Unauthorized Personnel</i>	192
<b>MEDIA PROTECTION (MP)</b>	<b>194</b>
P-MP-1: Media Protection Policy & Procedures	194
P-MP-2: Media Access	195
P-MP-3: Media Marking	196
P-MP-4: Media Storage	196
P-MP-5: Media Transport	197
P-MP-6: Media Sanitization	198
<i>P-MP-6(1): Media Sanitization   Review, Approve, Track, Document &amp; Verify</i>	199
<i>P-MP-6(2): Media Sanitization   Equipment Testing</i>	199
<i>P-MP-6(3): Media Sanitization   Non-Destructive Techniques</i>	200
<i>P-MP-6(7): Media Sanitization   Dual Authorization</i>	201
P-MP-7: Media Use	201
<b>PERSONNEL SECURITY (PS)</b>	<b>203</b>
P-PS-1: Personnel Security Policy & Procedures	203
P-PS-2: Position Risk Designation	204
P-PS-3: Personnel Screening	204
<i>P-PS-3(3): Personnel Screening   Information With Special Protection Measures</i>	205
P-PS-4: Personnel Termination	206
<i>P-PS-4(2): Personnel Termination   Automated Actions</i>	207
P-PS-5: Personnel Transfer	208
P-PS-6: Access Agreements	209
P-PS-7: External Personnel Security	209
P-PS-8: Personnel Sanctions	210
P-PS-9: Position Descriptions	211
<b>PHYSICAL &amp; ENVIRONMENTAL PROTECTION (PE)</b>	<b>213</b>
P-PE-1: Physical & Environmental Protection Policy & Procedures	213
P-PE-2: Physical Access Authorizations	214
P-PE-3: Physical Access Control	214
<i>P-PE-3(1): Physical Access Control   System Access</i>	216
P-PE-4: Access Control For Transmission	216
P-PE-5: Access Control For Output Devices	217
P-PE-6: Monitoring Physical Access	218
<i>P-PE-6(1): Monitoring Physical Access   Intrusion Alarms &amp; Surveillance Equipment</i>	219
<i>P-PE-6(4): Monitoring Physical Access   Monitoring Physical Access to Systems</i>	220
P-PE-8: Visitor Access Records	220
<i>P-PE-8(1): Visitor Access Records   Automated Records Maintenance &amp; Review</i>	221
<i>P-PE-8(3): Visitor Access Records   Limit Personally Identifiable Information Elements</i>	222
P-PE-9: Power Equipment & Cabling	223
P-PE-10: Emergency Shutoff	223
P-PE-11: Emergency Power	224
<i>P-PE-11(1): Emergency Power   Alternate Power Supply – Minimal Operational Capacity</i>	225
P-PE-12: Emergency Lighting	225
P-PE-13: Fire Protection	226
<i>P-PE-13(1): Fire Protection   Detection Devices – Automatic Activation &amp; Notification</i>	226
<i>P-PE-13(2): Fire Protection   Suppression Systems – Automatic Activation &amp; Notification</i>	227
P-PE-14: Environmental Controls	228

<i>P-PE-14(2): Environmental Controls   Monitoring with Alarms &amp; Notifications</i>	228
P-PE-15: Water Damage Protection	229
<i>P-PE-15(1): Water Damage Protection   Automation Support</i>	230
P-PE-16: Delivery & Removal	230
P-PE-17: Alternate Work Site	231
P-PE-18: Location of Information System Components	232
P-PE-20: Asset Monitoring & Tracking	233
<b>PERSONALLY IDENTIFIABLE INFORMATION (PII) PROCESSING &amp; TRANSPARENCY</b>	<b>235</b>
P-PT-1: Policy and Procedures	235
P-PT-2: Authority to Process PII	236
P-PT-3: PII Processing Purposes	236
P-PT-4: Consent	237
P-PT-5: Privacy Notice	238
<i>P-PT-5(2): Privacy Notice   Privacy Act Statements</i>	239
P-PT-6: System of Records Notice (SORN)	239
<i>P-PT-6(1): System of Records Notice (SORN)   Routine Uses</i>	240
<i>P-PT-6(2): System of Records Notice (SORN)   Exemption Rules</i>	241
P-PT-7: Specific Categories of PII	241
<i>P-PT-7(1): Specific Categories of PII   Social Security Numbers (SSN)</i>	242
<i>P-PT-7(2): Specific Categories of PII   First Amendment Information</i>	243
P-PT-8: Computer Matching Requirements	243
<b>TECHNICAL CONTROLS</b>	<b>245</b>
<b>ACCESS CONTROL (AC)</b>	<b>245</b>
P-AC-1: Access Control Policy & Procedures	245
P-AC-2: Account Management	246
<i>P-AC-2(1): Account Management   Automated System Account Management</i>	247
<i>P-AC-2(2): Account Management   Removal of Temporary / Emergency Accounts</i>	248
<i>P-AC-2(3): Account Management   Disable Inactive Accounts</i>	249
<i>P-AC-2(4): Account Management   Automated Audit Actions</i>	249
<i>P-AC-2(5): Account Management   Inactivity Logout</i>	250
<i>P-AC-2(7): Account Management   Privileged User Accounts</i>	251
<i>P-AC-2(9): Account Management   Restrictions on Use of Shared Groups &amp; Accounts</i>	251
<i>P-AC-2(11): Account Management   Usage Conditions</i>	252
<i>P-AC-2(12): Account Management   Account Monitoring for Atypical Usage</i>	253
<i>P-AC-2(13): Account Management   Disable Accounts for High-Risk Individuals</i>	253
P-AC-3: Access Enforcement	254
<i>P-AC-3(2): Access Enforcement   Dual Authorization</i>	255
<i>P-AC-3(14): Access Enforcement   Individual Access</i>	256
P-AC-4: Information Flow Enforcement	256
<i>P-AC-4(1): Information Flow Enforcement   Object Security &amp; Privacy Attributes</i>	257
<i>P-AC-4(4): Information Flow Enforcement   Content Check For Encrypted Data</i>	258
<i>P-AC-4(6): Information Flow Enforcement   Metadata</i>	259
<i>P-AC-4(8): Information Flow Enforcement   Security &amp; Privacy Policy Filters</i>	259
<i>P-AC-4(12): Information Flow Enforcement   Data Type Identifiers</i>	260
<i>P-AC-4(13): Information Flow Enforcement   Decomposition Into Policy-Relevant Subcomponents</i>	261
<i>P-AC-4(15): Information Flow Enforcement   Detection of Unsanctioned Information</i>	262
<i>P-AC-4(20): Information Flow Enforcement   Approved Solutions</i>	262
<i>P-AC-4(21): Information Flow Enforcement   Physical or Logical Separation for Information Flows</i>	263
P-AC-5: Separation of Duties	264
P-AC-6: Least Privilege	265
<i>P-AC-6(1): Least Privilege   Authorize Access to Security Functions</i>	266
<i>P-AC-6(2): Least Privilege   Non-Privileged Access for Non-Security Functions</i>	267
<i>P-AC-6(3): Least Privilege   Network Access to Privileged Commands</i>	268
<i>P-AC-6(5): Least Privilege   Privileged Accounts</i>	268
<i>P-AC-6(7): Least Privilege   Review of User Privileges</i>	269
<i>P-AC-6(8): Least Privilege   Privilege Levels for Code Execution</i>	270
<i>P-AC-6(9): Least Privilege   Auditing Use of Privileged Functions</i>	270

<i>P-AC-6(10): Least Privilege   Prohibit Non-Privileged Users from Executing Privileged Functions</i>	271
P-AC-7: Unsuccessful Logon Attempts	272
<i>P-AC-7(2): Unsuccessful Logon Attempts   Purge or Wipe Mobile Device</i>	273
P-AC-8: System Use Notification (Logon Banner)	273
P-AC-10: Concurrent Session Control	275
P-AC-11: Device Lock	275
<i>P-AC-11(1): Device Lock   Pattern-Hiding Displays</i>	276
P-AC-12: Session Termination	277
<i>P-AC-12(1): Session Termination   User-Initiated Logouts</i>	277
P-AC-14: Permitted Actions Without Identification or Authorization	278
P-AC-17: Remote Access	279
<i>P-AC-17(1): Remote Access   Monitoring &amp; Control</i>	280
<i>P-AC-17(2): Remote Access   Protection of Confidentiality &amp; Integrity Using Encryption</i>	280
<i>P-AC-17(3): Remote Access   Managed Access Control Points</i>	281
<i>P-AC-17(4): Remote Access   Privileged Commands &amp; Access</i>	282
<i>P-AC-17(9): Remote Access   Disconnect or Disable Remote Access</i>	283
P-AC-18: Wireless Access	283
<i>P-AC-18(1): Wireless Access   Authentication &amp; Encryption</i>	284
<i>P-AC-18(3): Wireless Access   Disable Wireless Networking</i>	285
<i>P-AC-18(4): Wireless Access   Restrict Configuration By Users</i>	285
<i>P-AC-18(5): Wireless Access   Antennas &amp; Transmission Power Levels</i>	286
P-AC-19: Access Control For Mobile Devices	287
<i>P-AC-19(5): Access Control For Mobile Devices   Full Device or Container-Based Encryption</i>	288
P-AC-20: Use of External Systems	289
<i>P-AC-20(1): Use of External Systems   Limits of Authorized Use</i>	290
<i>P-AC-20(2): Use of External Systems   Portable Storage Devices – Restricted Use</i>	290
<i>P-AC-20(3): Use of External Systems   Non-Organizationally Owned Systems – Restricted Use</i>	291
P-AC-21: Information Sharing	292
P-AC-22: Publicly Accessible Content	293
<b>AUDIT &amp; ACCOUNTABILITY (AU)</b>	<b>295</b>
P-AU-1: Audit & Accountability Policy & Procedures	295
P-AU-2: Event Logging	296
P-AU-3: Content of Audit Records	298
<i>P-AU-3(1): Content Of Audit Records   Additional Audit Information</i>	298
<i>P-AU-3(3): Content Of Audit Records   Limit Personally Identifiable Information Elements</i>	299
P-AU-4: Audit Log Storage Capacity	300
P-AU-5: Response To Audit Processing Failures	300
<i>P-AU-5(1): Response To Audit Processing Failures   Storage Capacity Warning</i>	301
<i>P-AU-5(2): Response To Audit Processing Failures   Real-Time Alerts</i>	302
P-AU-6: Audit Review, Analysis & Reporting	303
<i>P-AU-6(1): Audit Review, Analysis &amp; Reporting   Automated Process Integration</i>	304
<i>P-AU-6(3): Audit Review, Analysis &amp; Reporting   Correlate Audit Record Repositories</i>	304
<i>P-AU-6(4): Audit Review, Analysis &amp; Reporting   Central Review &amp; Analysis</i>	305
<i>P-AU-6(5) Audit Review, Analysis &amp; Reporting   Integrated Analysis of Audit Records</i>	306
<i>P-AU-6(6) Audit Review, Analysis &amp; Reporting   Correlation with Physical Monitoring</i>	306
<i>P-AU-6(7) Audit Review, Analysis &amp; Reporting   Permitted Actions</i>	307
P-AU-7: Audit Reduction & Report Generation	308
<i>P-AU-7(1): Audit Reduction &amp; Report Generation   Automatic Processing</i>	309
P-AU-8: Time Stamps	309
P-AU-9: Protection of Audit Information	310
<i>P-AU-9(2): Protection of Audit Information   Store on Separate Physical Systems or Components</i>	311
<i>P-AU-9(3): Protection of Audit Information   Cryptographic Protection</i>	311
<i>P-AU-9(4): Protection of Audit Information   Access by Subset of Privileged Users</i>	312
<i>P-AU-9(5): Protection of Audit Information   Dual Authorization</i>	313
P-AU-10: Non-Repudiation	313
P-AU-11: Audit Record Retention	314
P-AU-12: Audit Record Generation	315
<i>P-AU-12(1): Audit Record Generation   System-Wide &amp; Time-Correlated Audit Trail</i>	316



<i>P-AU-12(3): Audit Record Generation   Changes by Authorized Individuals</i>	316
P-AU-13: Monitoring For Information Disclosure	317
<b>CONFIGURATION MANAGEMENT (CM)</b>	<b>319</b>
P-CM-1: Configuration Management Policy & Procedures	319
P-CM-2: Baseline Configurations	320
<i>P-CM-2(2): Baseline Configuration   Automation Support for Accuracy &amp; Currency</i>	322
<i>P-CM-2(3): Baseline Configuration   Retention Of Previous Configurations</i>	323
<i>P-CM-2(7): Baseline Configuration   Configure Systems &amp; Components for High-Risk Areas</i>	323
P-CM-3: Configuration Change Control	324
<i>P-CM-3(1): Configuration Change Control   Automated Documentation, Notification &amp; Prohibition Of Changes</i>	325
<i>P-CM-3(2): Configuration Change Control   Testing, Validation &amp; Documentation of Changes</i>	326
<i>P-CM-3(4): Configuration Change Control   Security &amp; Privacy Representatives</i>	327
<i>P-CM-3(5): Configuration Change Control   Automated Security Response</i>	327
<i>P-CM-3(6): Configuration Change Control   Cryptography Management</i>	328
<i>P-CM-3(8): Configuration Change Control   Prevent or Restrict Configuration Changes</i>	328
P-CM-4: Impact Analysis	329
<i>P-CM-4(1): Impact Analysis   Separate Test Environments</i>	330
<i>P-CM-4(2): Impact Analysis   Verification of Controls</i>	330
P-CM-5: Access Restrictions For Change	331
<i>P-CM-5(1): Access Restrictions For Change   Automated Access Enforcement &amp; Audit Records</i>	332
<i>P-CM-5(4): Access Restrictions For Change   Dual Authorization (Two-Person Rule)</i>	332
<i>P-CM-5(5): Access Restrictions For Change   Privilege Limitation for Production &amp; Operation (Incompatible Roles)</i>	333
P-CM-6: Configuration Settings	334
<i>P-CM-6(1): Configuration Settings   Automated Management, Application &amp; Verification</i>	336
<i>P-CM-6(2): Configuration Settings   Respond To Unauthorized Changes</i>	336
P-CM-7: Least Functionality	337
<i>P-CM-7(1): Least Functionality   Periodic Review</i>	338
<i>P-CM-7(2): Least Functionality   Prevent Program Execution</i>	339
<i>P-CM-7(4): Least Functionality   Unauthorized Software (Blacklisting)</i>	339
<i>P-CM-7(5): Least Functionality   Authorized Software (Whitelisting)</i>	340
P-CM-8: System Component Inventory	341
<i>P-CM-8(1): System Component Inventory   Updates During Installation &amp; Removal</i>	342
<i>P-CM-8(2): System Component Inventory   Automated Maintenance</i>	342
<i>P-CM-8(3): System Component Inventory   Automated Unauthorized Component Detection</i>	343
<i>P-CM-8(4): System Component Inventory   Accountability Information</i>	344
P-CM-9: Configuration Management Plan	345
P-CM-10: Software Usage Restrictions	345
<i>P-CM-10(1): Software Usage Restrictions   Open Source Software</i>	346
P-CM-11: User-Installed Software	347
P-CM-12: Information Location	347
<i>P-CM-12(1): Information Location   Automated Tools To Support Information Location</i>	348
<b>IDENTIFICATION &amp; AUTHENTICATION (IA)</b>	<b>350</b>
P-IA-1: Identification & Authentication Policy & Procedures	350
P-IA-2: Identification & Authentication (Organizational Users)	351
<i>P-IA-2(1): Identification &amp; Authentication (Organizational Users)   Multi-Factor Authentication (MFA) to Privileged Accounts</i>	352
<i>P-IA-2(2): Identification &amp; Authentication (Organizational Users)   Multi-Factor Authentication (MFA) to Non-Privileged Accounts</i>	353
<i>P-IA-2(5): Identification &amp; Authentication (Organizational Users)   Individual Authentication With Group Authentication</i>	353
<i>P-IA-2(8): Identification &amp; Authentication (Organizational Users)   Access To Accounts - Replay Resistant</i>	354
<i>P-IA-2(12): Identification &amp; Authentication (Organizational Users)   Acceptance of PIV Credentials</i>	355
P-IA-3: Device Identification & Authentication	355
<i>P-IA-3(1): Device Identification &amp; Authentication   Cryptographic Bidirectional Authentication</i>	356
<i>P-IA-3(4): Device Identification &amp; Authentication   Device Attestation</i>	356
P-IA-4: Identifier Management (User Names)	357
<i>P-IA-4(4): Identifier Management   Identity User Status</i>	359
P-IA-5: Authenticator Management (Passwords)	359

<i>P-IA-5(1): Authenticator Management   Password-Based Authentication</i>	360
<i>P-IA-5(2): Authenticator Management   Public Key-Based Authentication</i>	362
<i>P-IA-5(6): Authenticator Management   Protection of Authenticators</i>	363
<i>P-IA-5(7): Authenticator Management   No Embedded Unencrypted Static Authenticators</i>	363
<i>P-IA-5(8): Authenticator Management   Multiple System Accounts</i>	364
<i>P-IA-5(13): Authenticator Management   Expiration of Cached Authenticators</i>	365
<i>P-IA-5(18): Authenticator Management   Password Managers</i>	365
P-IA-6: Authenticator Feedback	366
P-IA-7: Cryptographic Module Authentication	367
P-IA-8: Identification & Authentication (Non-Organizational Users)	367
<i>P-IA-8(1): Identification &amp; Authentication (Non-Organizational Users)   Acceptance of PIV Credentials from Other Organizations</i>	368
<i>P-IA-8(2): Identification &amp; Authentication (Non-Organizational Users)   Acceptance of External Authenticators</i>	369
<i>P-IA-8(4): Identification &amp; Authentication (Non-Organizational Users)   Use of Defined Profiles</i>	369
P-IA-10: Adaptive Authentication	370
P-IA-11: Re-Authentication	371
P-IA-12: Identity Proofing	371
<i>P-IA-12(2): Identity Proofing   Identity Evidence</i>	372
<i>P-IA-12(3): Identity Proofing   Identity Evidence Validation &amp; Verification</i>	373
<i>P-IA-12(4): Identity Proofing   In-Person Validation &amp; Verification</i>	373
<i>P-IA-12(5): Identity Proofing   Address Confirmation</i>	374
<b>MAINTENANCE (MA)</b>	<b>376</b>
P-MA-1: Maintenance Policy & Procedures	376
P-MA-2: Controlled Maintenance	376
<i>P-MA-2(2): Controlled Maintenance   Automated Maintenance Activities</i>	378
P-MA-3: Maintenance Tools	378
<i>P-MA-3(1): Maintenance Tools   Inspect Tools</i>	379
<i>P-MA-3(2): Maintenance Tools   Inspect Media</i>	380
<i>P-MA-3(3): Maintenance Tools   Prevent Unauthorized Removal</i>	380
P-MA-4: Non-Local Maintenance	381
<i>P-MA-4(3): Non-Local Maintenance   Comparable Security &amp; Sanitization</i>	382
<i>P-MA-4(6): Non-Local Maintenance   Cryptographic Protection</i>	383
P-MA-5: Maintenance Personnel	383
<i>P-MA-5(1): Maintenance Personnel   Individuals Without Appropriate Access</i>	384
P-MA-6: Timely Maintenance	385
<b>SYSTEM &amp; COMMUNICATION PROTECTION (SC)</b>	<b>386</b>
P-SC-1: System & Communication Policy & Procedures	386
P-SC-2: Separation of System & User Functionality	387
P-SC-3: Security Function Isolation	387
P-SC-4: Information In Shared Resources	388
P-SC-5: Denial of Service (DoS) Protection	389
P-SC-6: Resource Availability	390
P-SC-7: Boundary Protection	390
<i>P-SC-7(3): Boundary Protection   Access Points</i>	392
<i>P-SC-7(4): Boundary Protection   External Telecommunications Services</i>	392
<i>P-SC-7(5): Boundary Protection   Deny by Default - Allow by Exception (Access Control List)</i>	393
<i>P-SC-7(7): Boundary Protection   Split Tunneling for Remote Devices</i>	394
<i>P-SC-7(8): Boundary Protection   Route Traffic To Authenticated Proxy Servers</i>	394
<i>P-SC-7(10): Boundary Protection   Prevent Exfiltration</i>	395
<i>P-SC-7(12): Boundary Protection   Host-Based Protection</i>	396
<i>P-SC-7(13): Boundary Protection   Isolation of Security Tools, Mechanisms &amp; Support Components (Security Subnet)</i>	396
<i>P-SC-7(18): Boundary Protection   Fail Secure</i>	397
<i>P-SC-7(20): Boundary Protection   Dynamic Isolation &amp; Segregation (Sandboxing)</i>	399
<i>P-SC-7(21): Boundary Protection   Isolation of System Components (DMZ)</i>	399
<i>P-SC-7(22): Boundary Protection   Separate Subnets for Connecting To Different Security Domains</i>	400
<i>P-SC-7(24): Boundary Protection   Personally Identifiable Information</i>	400
P-SC-8: Transmission Confidentiality & Integrity	401

<i>P-SC-8(1): Transmission Confidentiality &amp; Integrity   Cryptographic or Alternate Physical Protection</i>	402
<i>P-SC-8(4): Transmission Confidentiality &amp; Integrity   Conceal or Randomize Communications</i>	403
P-SC-10: Network Disconnect	404
P-SC-12: Cryptographic Key Establishment & Management	404
<i>P-SC-12(1): Cryptographic Key Establishment &amp; Management   Availability</i>	405
<i>P-SC-12(2): Cryptographic Key Establishment &amp; Management   Symmetric Keys</i>	406
<i>P-SC-12(3): Cryptographic Key Establishment &amp; Management   Asymmetric Keys</i>	406
P-SC-13: Cryptographic Protection	407
P-SC-15: Collaborative Computing Devices & Applications	408
P-SC-17: Public Key Infrastructure (PKI) Certificates	409
P-SC-18: Mobile Code	410
<i>P-SC-18(3): Mobile Code   Prevent Downloading &amp; Execution</i>	411
P-SC-20: Secure Name / Address Resolution Service (Authoritative Source)	411
P-SC-21: Secure Name / Address Resolution Service (Recursive or Caching Resolver)	412
P-SC-22: Architecture & Provisioning For Name / Address Resolution Service	413
P-SC-23: Session Authenticity	414
<i>P-SC-23(1): Session Authenticity   Invalidate Session Identifiers at Logout</i>	414
P-SC-24: Fail In Known State	415
P-SC-25: Thin Nodes	415
P-SC-26: Decoys	416
P-SC-27: Platform-Independent Applications	417
P-SC-28: Protection of Information At Rest	418
<i>P-SC-28(1): Protection of Information at Rest   Cryptographic Protection</i>	418
<i>P-SC-28(2): Protection of Information at Rest   Offline Storage</i>	419
P-SC-29: Heterogeneity	420
<i>P-SC-29(1): Heterogeneity   Virtualization Techniques</i>	421
P-SC-30: Concealment & Misdirection	421
<i>P-SC-30(2): Concealment and Misdirection   Randomness</i>	422
<i>P-SC-30(3): Concealment and Misdirection   Change Processing &amp; Storage Locations</i>	423
P-SC-38: Operations Security	423
P-SC-39: Process Isolation	424
P-SC-44: Detonation Chambers	425
P-SC-45: System Time Synchronization	426
<i>P-SC-45(1): System Time Synchronization   Synchronization With Authoritative Time Source</i>	426
P-SC-46: Cross Domain Policy Enforcement	427
P-SC-47: Alternate Communications Paths	428
P-SC-49: Hardware-Enforced Separation & Policy Enforcement	428
<b>SYSTEM &amp; INFORMATION INTEGRITY (SI)</b>	<b>430</b>
P-SI-1: System & Information Integrity Policy & Procedures	430
P-SI-2: Flaw Remediation (Software Patching)	431
<i>P-SI-2(2): Flaw Remediation   Automated Flaw Remediation Status</i>	432
<i>P-SI-2(3): Flaw Remediation   Time To Remediate Flaws &amp; Benchmarks For Corrective Action</i>	433
P-SI-3: Malicious Code Protection (Malware)	433
P-SI-4: System Monitoring	435
<i>P-SI-4(1): System Monitoring   System-Wide Intrusion Detection System</i>	436
<i>P-SI-4(2): System Monitoring   Automated Tools for Real-Time Analysis</i>	436
<i>P-SI-4(4): System Monitoring   Inbound &amp; Outbound Communications Traffic</i>	437
<i>P-SI-4(5): System Monitoring   System Generated Alerts</i>	438
<i>P-SI-4(7): Information System Monitoring   Automated Response To Suspicious Events</i>	438
<i>SI-4(10): System Monitoring   Visibility of Encrypted Communications</i>	439
<i>P-SI-4(11): System Monitoring   Analyze Communications Traffic Anomalies</i>	440
<i>P-SI-4(12): System Monitoring   Automated Organization-Generated Alerts</i>	440
<i>P-SI-4(13): System Monitoring   Analyze Traffic &amp; Event Patterns</i>	441
<i>P-SI-4(14): System Monitoring   Wireless Intrusion Detection</i>	442
<i>P-SI-4(16): System Monitoring   Correlate Monitoring Information</i>	442
<i>P-SI-4(18): System Monitoring   Analyze Traffic &amp; Covert Exfiltration</i>	443
<i>P-SI-4(19): System Monitoring   Individuals Posing Greater Risk</i>	444
<i>P-SI-4(20): System Monitoring   Privileged Users</i>	444

<i>P-SI-4(22): System Monitoring   Unauthorized Network Services</i>	445
<i>P-SI-4(23): System Monitoring   Host-Based Devices</i>	446
<i>P-SI-4(24): System Monitoring   Indicators of Compromise (IOC)</i>	446
P-SI-5: Security Alerts, Advisories & Directives	447
<i>P-SI-5(1): Security Alerts, Advisories &amp; Directives   Automated Alerts &amp; Advisories</i>	448
P-SI-6: Security & Privacy Functionality Verification	449
P-SI-7: Software, Firmware & Information Integrity	449
<i>P-SI-7(1): Software, Firmware &amp; Information Integrity   Integrity Checks</i>	450
<i>P-SI-7(2): Software, Firmware &amp; Information Integrity   Automated Notifications of Integrity Violations</i>	451
<i>P-SI-7(5): Software, Firmware &amp; Information Integrity   Automated Response to Integrity Violations</i>	452
<i>P-SI-7(6): Software &amp; Information Integrity   Cryptographic Protection</i>	452
<i>P-SI-7(7): Software, Firmware &amp; Information Integrity   Integration of Detection &amp; Response</i>	453
<i>P-SI-7(9): Software &amp; Information Integrity   Verify Boot Process</i>	454
<i>P-SI-7(10): Software, Firmware &amp; Information Integrity   Protection of Boot Firmware</i>	454
<i>SI-7(15): Software, Firmware &amp; Information Integrity   Code Authentication</i>	455
P-SI-8: Spam Protection	455
<i>P-SI-8(2): Spam Protection   Automatic Updates</i>	456
P-SI-10: Input Data Validation	457
P-SI-11: Error Handling	457
P-SI-12: Information Output Handling & Retention	458
<i>P-SI-12(1): Information Management &amp; Retention   Limit Personally Identifiable Information Elements</i>	459
<i>P-SI-12(2): Information Management &amp; Retention   Minimize Personally Identifiable Information In Testing, Training &amp; Research</i>	460
<i>P-SI-12(3): Information Management &amp; Retention   Information Disposal</i>	461
P-SI-14: Non-Persistence	462
<i>P-SI-14(1): Non-Persistence   Refresh from Trusted Sources</i>	462
<i>SI-14(2): Non-Persistence   Non-Persistent Information</i>	463
<i>SI-14(3): Non-Persistence   Non-Persistent Connectivity</i>	464
P-SI-16: Memory Protection	465
P-SI-18: Personally Identifiable Information Quality Operations	465
<i>P-SI-18(4): Personally Identifiable Information Quality Operations   Individual Requests</i>	466
P-SI-19: De-Identification	467
P-SI-20: Tainting	468

---

**GLOSSARY: ACRONYMS & DEFINITIONS** **469**

**ACRONYMS** **469**

**DEFINITIONS** **469**

---

**RECORD OF CHANGES** **470**



## 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).

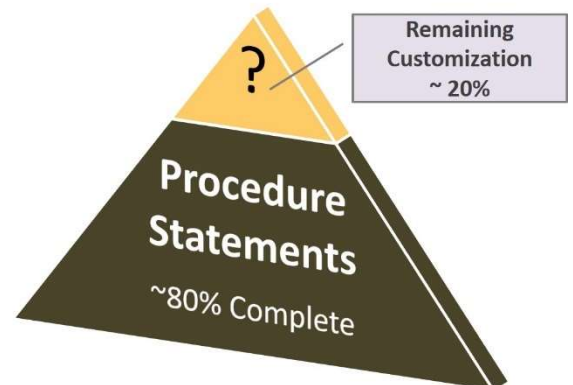
### OVERVIEW

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 reassess 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.

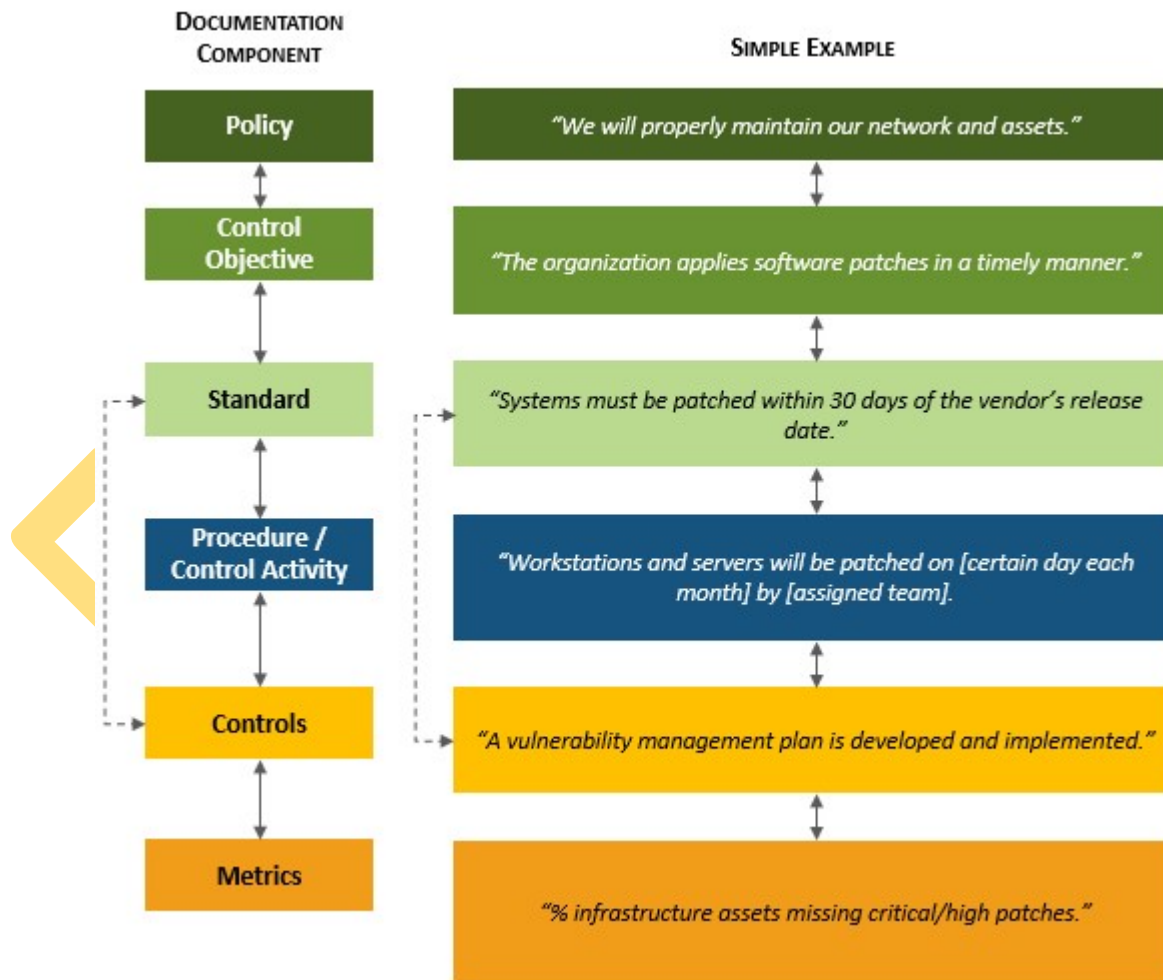
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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

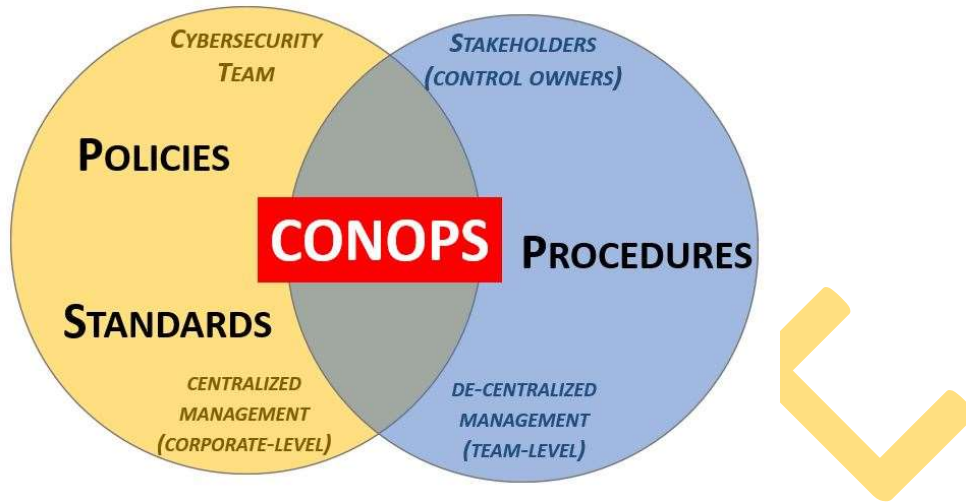
<sup>3</sup> NIST SP 800-171A assessment criteria 3.4.1[a] & 3.4.1[c]

<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**

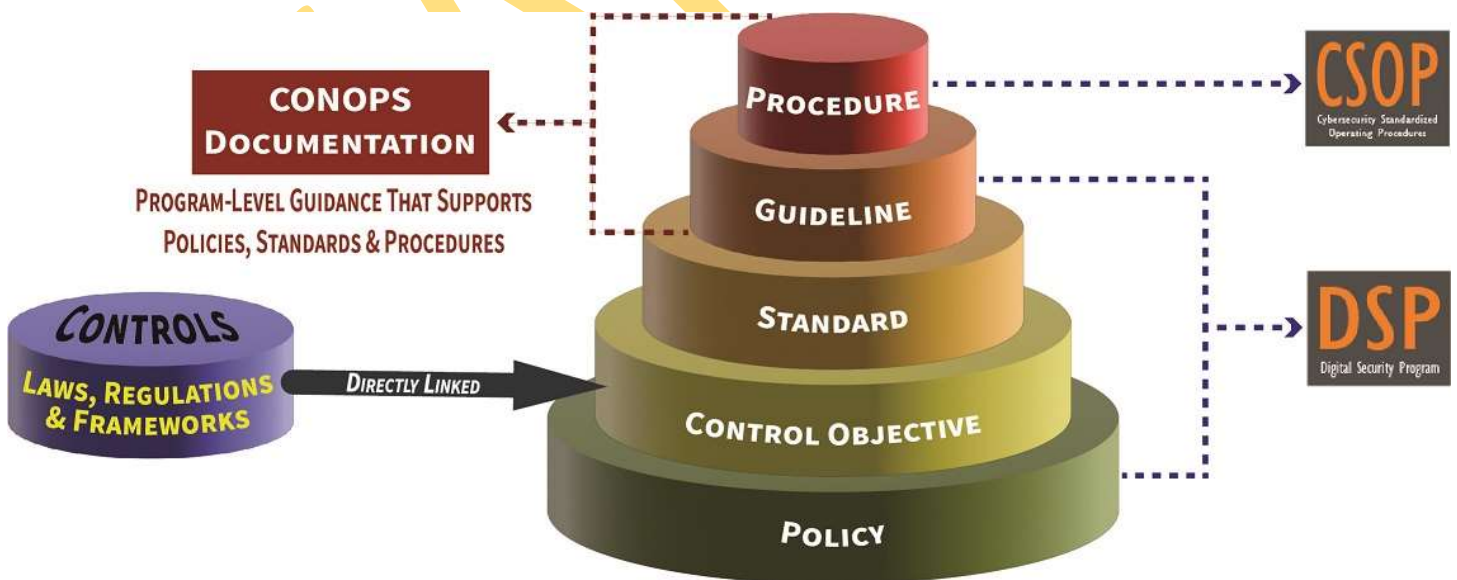
While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with ComplianceForge’s [NIST SP 800-53-based Cybersecurity & Data Protection Program \(CDPP\)](#) that contains policies, control objectives, standards and guidelines.



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

## P-PM-2: INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

**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:** Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement and maintain an organization-wide information security program.<sup>6</sup>

**Procedure / Control Activity:** The Human Resources (HR) department, in conjunction with Executive Cyber Leadership [OV-EXL-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

- (1) Leverages the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CSF)<sup>7</sup> for identifying necessary roles and responsibilities, including the Chief Information Security Officer (CISO).
- (2) Utilizes existing HR processes to assign formal roles and responsibilities to the CISO to perform or delegate the following cybersecurity management responsibilities:
  - a. Establish, document and distribute security policies and procedures;
  - b. Monitor and analyze security alerts and information;
  - c. Distribute and escalate security alerts to appropriate personnel;
  - d. Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
  - e. Administer user accounts, including additions, deletions and modifications; and
  - f. Monitor and control all access to data.
- (3) Provides written notification to the employee assigned the role of CISO.
- (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-PM-3: INFORMATION SECURITY AND PRIVACY RESOURCES

**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?

<sup>6</sup> NIST SP 800-53 Rev 5 control PM-2

<sup>7</sup> NIST NICE - <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

## 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



**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 and technical means to conducts periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.<sup>239</sup>
- (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-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>240</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

<sup>239</sup> NIST SP 800-171A assessment criteria 3.6.3

<sup>240</sup> NIST SP 800-53 Rev 5 control IR-3(2)

- 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>241</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;
- 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>242</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>243</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>244</sup>
  - b. Detection;<sup>245</sup>
  - c. Analysis;<sup>246</sup>
  - d. Containment;<sup>247</sup> and
  - e. Recovery.<sup>248</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

<sup>241</sup> NIST SP 800-53 Rev 5 control IR-4

<sup>242</sup> NIST SP 800-171A assessment criteria 3.6.1[a]

<sup>243</sup> NIST SP 800-171A assessment criteria 3.6.1[g]

<sup>244</sup> NIST SP 800-171A assessment criteria 3.6.1[b]

<sup>245</sup> NIST SP 800-171A assessment criteria 3.6.1[c]

<sup>246</sup> NIST SP 800-171A assessment criteria 3.6.1[d]

<sup>247</sup> NIST SP 800-171A assessment criteria 3.6.1[e]

<sup>248</sup> NIST SP 800-171A assessment criteria 3.6.1[f]

- 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>249</sup>

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

- (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(2): INCIDENT HANDLING | DYNAMIC RECONFIGURATION**

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: Include organization-defined types of dynamic reconfiguration for organization-defined system components as part of the incident response capability.<sup>250</sup>

Procedure / Control Activity: System Administrator [OM-ADM-001], in conjunction with Asset Owner [XX-AST-001], Crisis Management Specialist [XX-CON-001], Disaster Recovery Team Leader [XX-CON-003] and Business Continuity Team Leader [XX-CON-005]:

- (1) Develops specific use cases where dynamic reconfiguration is appropriate that includes:
  - a. Stopping an active attack;
  - b. Misdirecting attackers; and
  - c. Isolating systems, thus limiting the extent of the damage from breaches or compromises.
- (2) Implements appropriate administrative and technical means to employ automated mechanisms that enable dynamic reconfiguration of systems as part of incident response remediation actions that includes:
  - a. Changes to router or firewall Access Control Lists (ACLs); and

<sup>249</sup> NIST SP 800-53 Rev 5 control IR-4(1)

<sup>250</sup> NIST SP 800-53 Rev 5 control IR-4(2)

- b. Intrusion Detection / Prevention System (IDS/IPS) parameters.
- (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(3): INCIDENT HANDLING | CONTINUITY OF OPERATIONS**

**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:** Identify classes of incidents and take organization-defined actions in response to those incidents to ensure continuation of organizational mission and business functions.<sup>251</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) Leverages the Integrated Incident Response Program (IIRP) to categorize cybersecurity incidents based on each category’s potential to escalate and different handling procedures:

#	Threat	Category	Category Description
0	Training	<b>Simulated Incident</b> (Training & Exercises)	This category is used during exercises and approved testing of internal/external network defenses or responses.
1	Illegal Content or Activities	<b>Illegal Content</b>	This category is used for any data that is illegal to have in possession. This includes illegal content such as <u>child pornography</u> or <u>classified information on unclassified systems</u> .
2		<b>Criminal Conduct</b>	This category is used for any incident that would be considered criminal conduct. This includes <u>embezzlement</u> , <u>corporate espionage</u> , <u>terrorism/national security threats</u> , <u>fraud</u> , <u>violence</u> or other conduct that would constitute a <u>criminal felony or misdemeanor charge</u> .
3	Safety	<b>Technology Compromise</b>	This category is used for any incident that has <u>safety implications</u> from the compromise of the technology to be used in a manner it was not designed for. This includes categories of technologies that includes <u>Operational Technology (OT)</u> and <u>Internet of Things (IoT)</u> .

<sup>251</sup> NIST SP 800-53 Rev 5 control IR-4(3)

4	Confidentiality	Breach of Sensitive Data	This category is used for any incident that has involves the <u>unauthorized disclosure or compromise of sensitive data</u> .  This includes sensitive <u>Personal Data (PD)</u> and <u>Intellectual Property (IP)</u> .
5	Nefarious Activity	Malware	This category is used for malware-related incidents.  Any software code intentionally created or introduced into multiple systems for the distinct purpose of causing hard or loss to the computer system, its data or other resources (e.g., spyware, adware, viruses, Trojans, worms, etc.).
6		Host / Application Compromise	This is a <u>known or suspected compromise</u> that is not directly related to malware.  A successful event of this nature means the <u>attacker has total control over the host or application</u> and access to any and all data stored on it or on systems that trust the compromised host or application.  This may be from a <u>privilege escalation attack</u> .
7		Denial of Service (DoS)	This is a known or suspected <u>Denial of Service (DoS) attack</u> .  A successful event of this nature means the attacker(s) successfully denied access to either the entire network, a portion of the network or to critical service(s) / website(s).
8	Lost / Stolen Asset	Lost / Stolen IT Asset	This category is used to respond to any <u>lost or stolen IT equipment</u> (e.g., laptops, tablets, computers, servers, media, tapes, etc.)
9	Poor Security Practice	Poor Security Practice	This category is used for any suspected incident involving <u>misconfigurations, poor cybersecurity practices &amp; policy violations</u> .
10	Unknown / Other	Unknown / Other (Under Investigation)	This category is used if the <u>situation is unclear and categorization cannot be made</u> .  This is meant to be a "placeholder" category until the threat or situation is investigated and a final determination has been made, so that the incident can be properly categorized.

- (2) Implements appropriate administrative and technical means to employ the IIRP to ensure users understand the different categories of incidents and the actions required to be taken, per ACME's Incident Response Plan (IRP).
- (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(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?