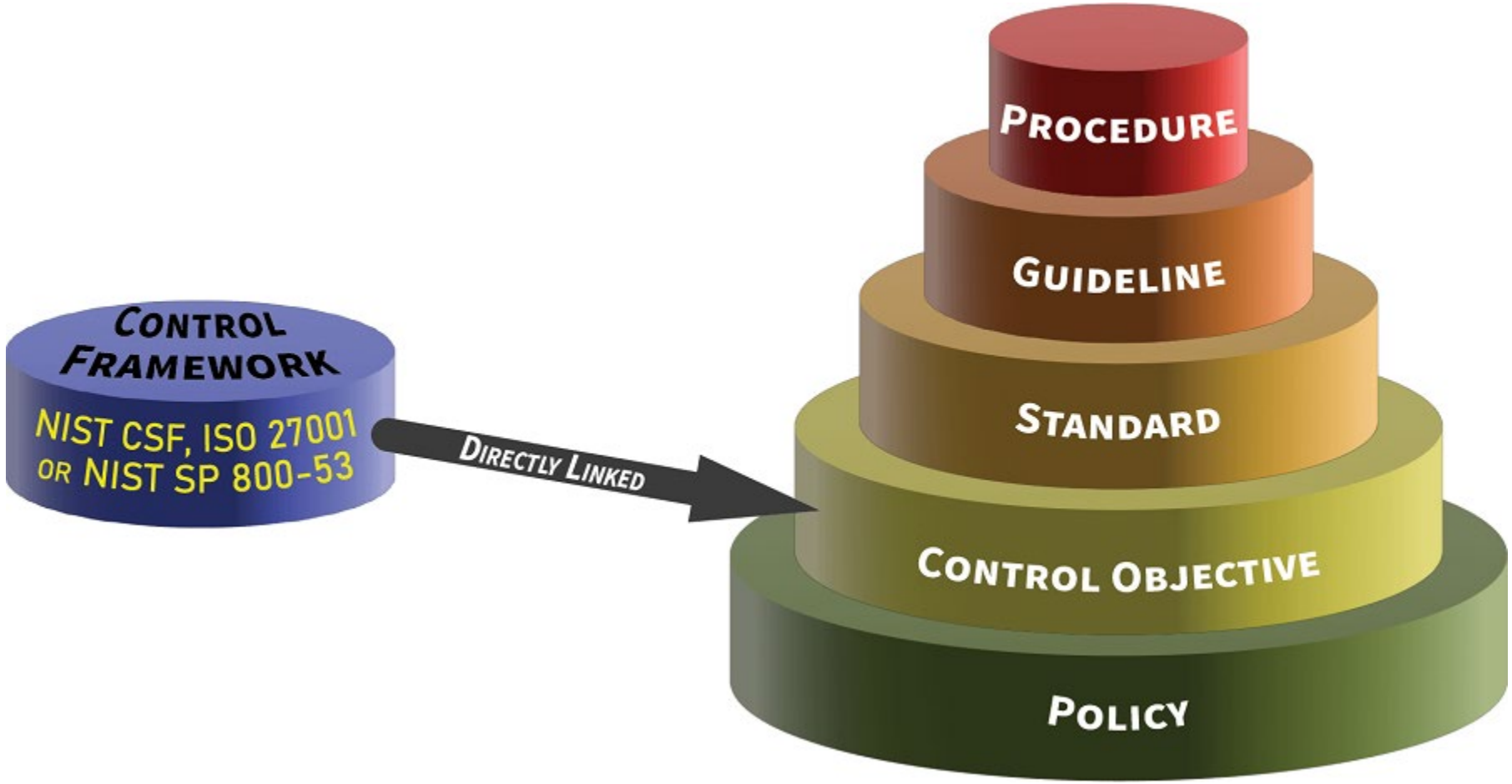
COMPLIANCE FORGE

Cybersecurity Documentation Examples

- Policies
- Control Objectives
- Standards
- Guidelines
- Controls
- Procedures
- Metricts

Simplified Cybersecurity Documentation Hierarchy

Cybersecurity documentation is meant to be hierarchical. This foundation starts with the policy and builds from there with supporting elements (e.g., standards, guidelines, etc.) that come together to demonstrate appropriate evidence of due diligence and due care.



Simplified Cybersecurity Documentation Hierarchy

Policies address the ***"why do we need to do this?"*** question. Policies are not meant to be prescriptive but provide an overall direction for the organization (e.g., high level statement of management intent).

Control Objectives address the ***"what are the leading practices?"*** question that identifies applicable requirements that the organization needs to address (e.g., laws, regulations or other compliance obligations).

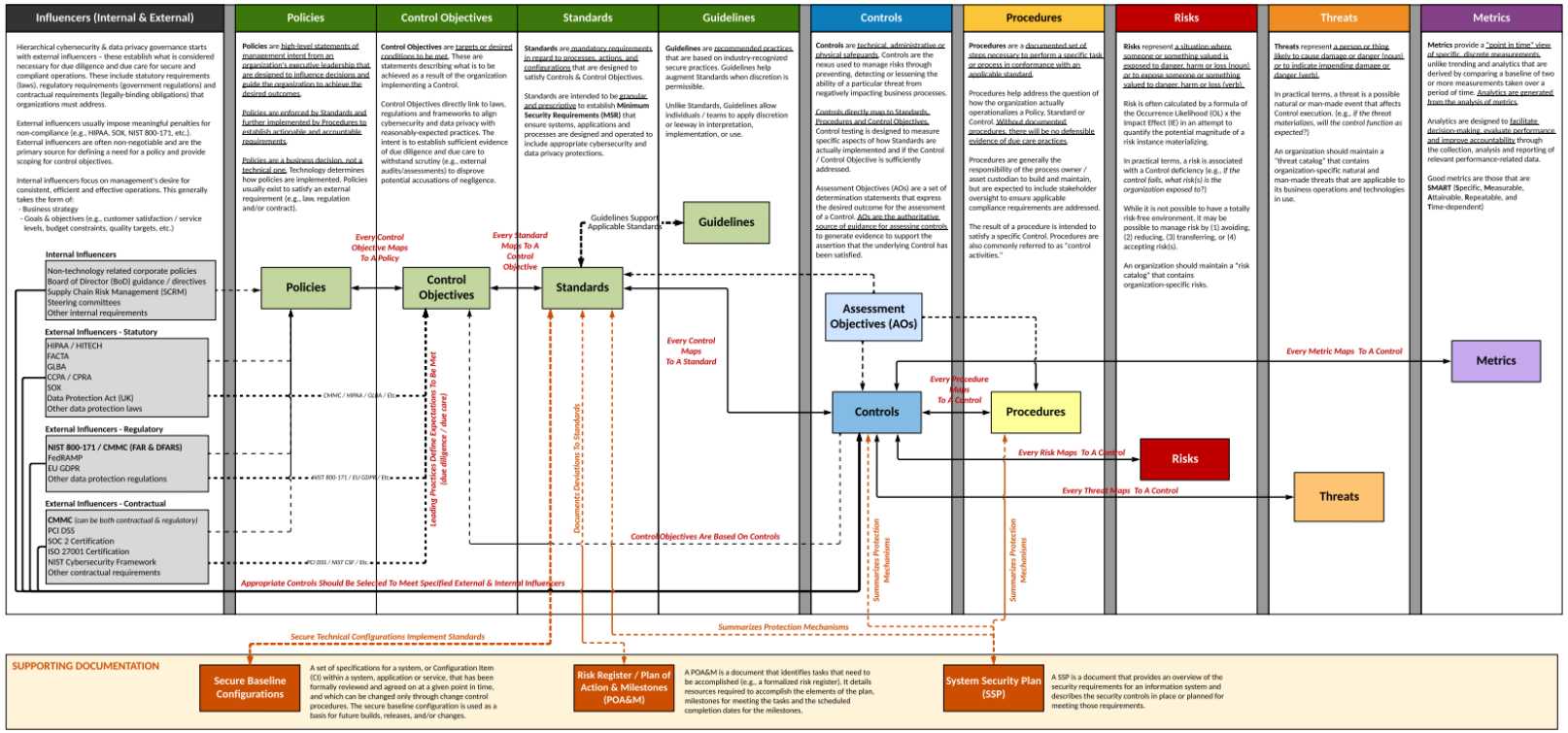
Standards address the ***"what is the requirement?"*** question and are intended to be granular in nature to provide objective requirements (e.g., 12-character passwords, requirements for Multi-Factor Authentication (MFA), etc.).

Procedures address the ***"how do we actually do this?"*** question. These are often referred to Control Activities, but many organizations document them as Standardized Operating Procedures or SOPs.

Guidelines help augment Standards when discretion is permissible and serve as useful guidance.

A Picture Is Worth 1,000+ Words

In cybersecurity compliance, words matter. Understanding cybersecurity documentation dependencies is important. The swim lane diagram shown below helps visualize how cybersecurity documentation is meant to work together, as well as provide authoritative definitions for documentation elements from NIST, ISO, ISACA and AICPA:



Download from: https://complianceforge.com/grc/hierarchical-cybersecurity-governance-framework/

CYBERSECURITY DOCUMENTATION EXAMPLES

Policy | Control Objective | Standard | Guideline | Control | Procedure | Metric

POLICY: A policy is a high-level statement of management's intent (e.g., no more than 1-3 sentences are necessary) where the policy should be clear and concise. It is a formally-established requirement to guide decisions and achieve rational outcomes.

EXAMPLE 1 - CONFIGURATION MANAGEMENT (CFG)*

Policy: ACME shall ensure all technology platforms used in support of its business operations adhere with industry-recognized secure configuration management practices. Current and accurate inventories of technology platforms shall be maintained so applicable secure configuration settings can be enforced on those technology platforms.

EXAMPLE 2 - CONTINUOUS MONITORING (MON)*

Policy: ACME shall achieve and maintain situational awareness through comprehensive and ongoing monitoring activities to help ensure the security and resilience of its technology infrastructure against both physical and cyber threats. Technology assets shall be configured according to secure configuration management requirements to enable the capture of relevant security event logs. A centralized log analysis capability shall be used to identify anomalous behavior and support incident response operations so that appropriate steps can be taken to remediate potential incidents.

Policies are from the **Digital Security Program (DSP)*

CYBERSECURITY DOCUMENTATION EXAMPLES

Policy | **Control Objective** | Standard | Guideline | Control | Procedure | Metric

CONTROL OBJECTIVE: A control objective provides a specific target against which to evaluate the effectiveness of controls. It is a target or desired condition to be met.

CFG-03 – LEAST FUNCTIONALITY*

Control Objective: The organization configures systems to provide only essential capabilities and specifically prohibits or restricts the use of ports, protocols, and / or services.

CFG-03 External Influencers: ISO 27002-2022: 8.3, 8.9, 8.12 | NIST SP 800-53 R5: CM-7 | NIST SP 800-171 R2: 3.4.6 | NIST SP 800-171 R3: 03.04.02.a, 03.04.06.a, 03.04.06.b, 03.04.06.d, 03.04.08.a | FAR 52.204-21(b)(1)(ii) | NIST CSF 2.0: PR.PS-05

MON-02 – CENTRALIZED EVENT LOG COLLECTION*

Control Objective: The organization:

- Monitors events on systems in accordance with organization-defined monitoring objectives and detects system attacks;
- Identifies unauthorized use of systems; and
- Heightens the level of system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals or other organizations, based on credible sources of information.
- Determines, based on a risk assessment and mission / business needs, that the system must be capable of auditing events;
- Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and
- Provides a rationale for why the list of auditable events is deemed to be adequate to support after-the-fact investigations of security incidents.

MON-02 External Influencers: ISO 27002-2022: 8.15 | NIST SP 800-53 R5: AU-2, AU-2(3), AU-6, IR-4(4), SI-4 | NIST SP 800-171 R2: 3.3.1, 3.3.3, 3.3.5, 3.3.6, 3.3.8, 3.3.9 | NIST SP 800-171 R3: 03.03.05.a, 03.03.05.c | NIST CSF 2.0: DE.AE-03, DE.AE-06

Control Objectives are from the **Digital Security Program (DSP)*

CYBERSECURITY DOCUMENTATION EXAMPLES

Policy | Control Objective | **Standard** | Guideline | Control | Procedure | Metric

STANDARD: Standards are granular requirements that support Policies. These satisfy Control Objectives regarding processes, actions and configurations.

CFG-03 – LEAST FUNCTIONALITY*

Standard: ACME utilizes the "principle of least privilege," which states that only the minimum access and functionality necessary to perform an operation should be granted and only for the minimum amount of time necessary. Asset custodians are required to:

(a) Identify and remove insecure services, protocols and ports;
(b) Enable only necessary and secure services, protocols and daemons, as required for the function of the system;
(c) Implement security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.);
(d) Verify services, protocols and ports are documented and properly implemented by examining device settings; and
(e) Remove all unnecessary functionality, such as:
1. Scripts;
2. Drivers;
3. Features;
4. Subsystems;
5. File systems; and
6. Unnecessary web servers.

MON-02: CENTRALIZED EVENT LOG COLLECTION*

Standard: Asset custodians are required to configure all systems, devices and applications to implement automated audit trails for all system components and automatically forward security-related event logs to a centralized log collector or Security Incident Event Management (SIEM) solution to allow ACME security personnel to reconstruct the following events:

(a) All individual user accesses to sensitive data (e.g., payment card data, SSNs, financial accounts, etc.);
(b) All actions taken by any individual with root or administrative privileges;
(c) Access to all audit trails;
(d) Invalid logical access attempts;
(e) Use of and changes to identification and authentication mechanisms, including but not limited to:
1. Creation of new accounts and elevation of privileges; and
2. All changes, additions or deletions to accounts with root or administrative privileges;
(f) Initialization, stopping or pausing of the audit logs; and
(g) Creation and deletion of system-level objects.

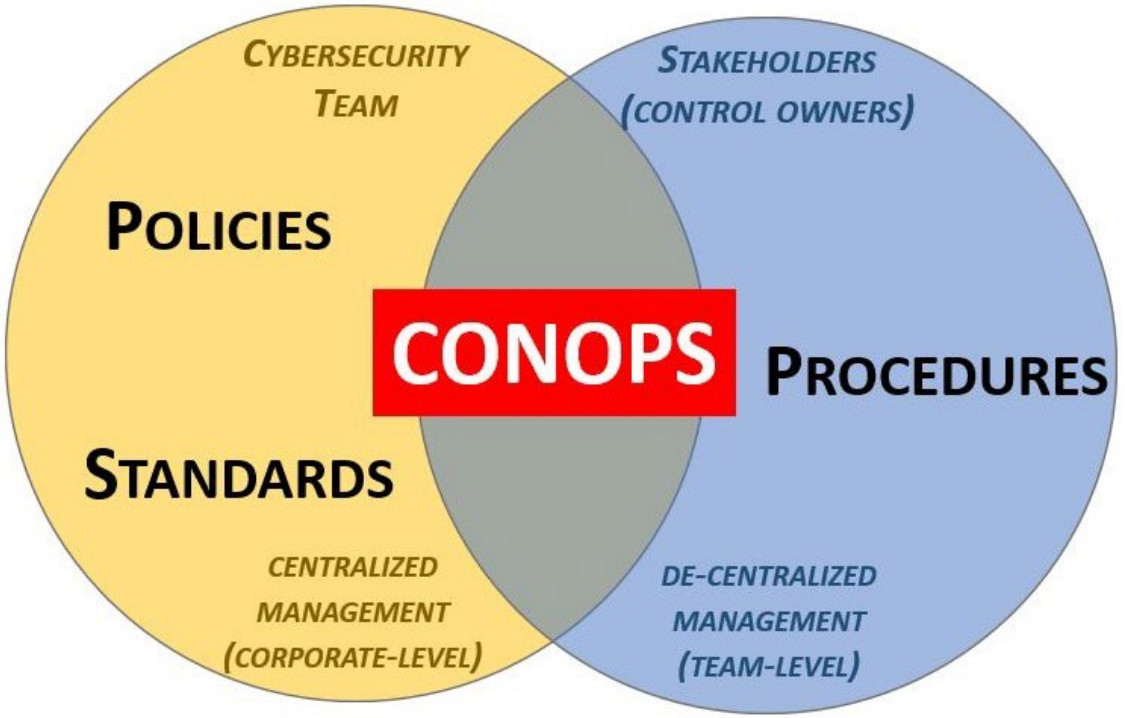
Standards are from the **Digital Security Program (DSP)*

Cybersecurity Documentation Examples

Policy | Control Objective | **Standard** | Guideline | Control | Procedure | Metric

Within the context of standards falls the concept of "program level guidance" documentation. A Concept of Operations (**CONOPS**) is a user-oriented guidance document that describes the mission, operational objectives and overall expectations from an integrated systems point of view, without being overly technical or formal.

A CONOPS straddles the territory between an organization's centrally-managed policies / standards and its decentralized procedures. The CONOPS serves as expert-level guidance that is meant to run a specific function within the cybersecurity department (e.g., risk management, vulnerability management, etc.).



CYBERSECURITY DOCUMENTATION EXAMPLES

Policy | Control Objective | **Standard** | Guideline | Control | Procedure | Metric

Several ComplianceForge documents are essentially CONOPS documents, where CONOPS are more conceptual than procedures and are focused on providing program-level guidance.

Examples of where a CONOPS is useful for providing program-level guidance:

- Risk management (e.g., Risk Management Program)
- Vulnerability management (e.g., Vulnerability & Patch Management Program)
- Incident response (e.g., Integrated Incident Response Program)
- Business Continuity / Disaster Recovery (e.g., Continuity of Operations Plan)
- Data privacy (e.g., Data Privacy Program)
- Secure Engineering (e.g., Secure Engineering & Data Privacy Program)
- Pre-production testing (e.g., Information Assurance Program)
- Supply Chain Risk Management (SCRM) (e.g., C-SCRM Strategy & Implementation Plan)

Cybersecurity Documentation Examples

Policy | Control Objective | Standard | **Guideline** | Control | Procedure | Metric

GUIDELINE: Guidelines are recommended, but not required, practices. Guidelines can be used to augment Standards when discretion is permissible.

CFG-03 – Least Functionality*

Guideline: Asset custodians should review functions and services of systems, to determine which functions and services are candidates for elimination (e.g., Instant Messaging, SMS, auto-execute and file sharing). ACME may utilize network scanning tools, intrusion detection and prevention systems and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols and services.

MON-02 – Centralized Event Log Collection*

Guideline: Monitoring is necessary to ensure that only authorized processes are being performed. The level of monitoring required will depend upon the business function in question. All monitoring activities will be formally authorized by management. System monitoring includes external and internal monitoring and the collection of monitoring data will be limited to justifiable business and legal purposes.

- External monitoring includes the observation of events occurring at the system boundary (e.g., part of perimeter defense and boundary protection).
- Internal monitoring includes the observation of events occurring within the system.

Guidelines are from the **Digital Security Program (DSP)*

CYBERSECURITY DOCUMENTATION EXAMPLES

Policy | Control Objective | Standard | Guideline | **Control** | Procedure | Metric

CONTROL: Controls are technical, administrative and/or physical safeguard that exists to prevent, detect or lessen the impact or ability of a threat to exploit a vulnerability. ISO 27002 and NIST SP 800-53 are examples of a "controls catalog," which is a collection of security and privacy controls.

CFG-03 – LEAST FUNCTIONALITY*

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

MON-02 – CENTRALIZED EVENT LOG COLLECTION*

Control: Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.

Controls are from the **Secure Controls Framework (SCF)*

Policy | Control Objective | Standard | Guideline | Control | **Procedure** | Metric

PROCEDURE: Procedures are a formal method of doing something, based on a series of actions that are conducted in a certain order or manner.

P-CFG-03 – LEAST FUNCTIONALITY*

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

(1) Uses vendor-recommended settings and industry-recognized secure practices to ensure configuration parameters limit privileges to the minimum amount necessary for the user/service to perform needed functions.
(2) Identifies and removes insecure services, protocols, and ports.
(3) Enables only necessary and secure services, protocols, and daemons, as required for the function of the system.
(4) Implements security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.).
(5) Verifies services, protocols, and ports are documented and properly implemented by examining firewall and router configuration settings.
(6) Removes all unnecessary functionality, such as:
  a. Scripts;
  b. Drivers;
  c. Features;
  d. Subsystems;
  e. File systems; and
  f. Unnecessary web servers.
(7) Utilizes network scanning tools, intrusion detection and prevention systems, and endpoint protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.
(8) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  a. Distributes copies of the change to key personnel; and
  b. Communicates the changes and updates to key personnel.
(9) If necessary, requests corrective action to address identified deficiencies.
(10) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(11) If necessary, documents the results of corrective action and notes findings.
(12) If necessary, requests additional corrective action to address unremediated deficiencies.

Procedures are from the **Cybersecurity Standardized Operating Procedures (CSOP)*

Policy | Control Objective | Standard | Guideline | Control | **Procedure** | Metric

PROCEDURE: Procedures are a formal method of doing something, based on a series of actions that are conducted in a certain order or manner.

P-MON-02 – CENTRALIZED EVENT LOG COLLECTION*

Procedure: Cyber Defense Analyst [PR-CDA-001], in conjunction with Systems Security Developer [SP-SYS-001], Network Operations Specialist [OM-NET-001], System Administrator [OM-ADM-001] and Cyber Defense Incident Responder [PR-CIR-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to utilize the Security Incident Event Manger (SIEM) log review process to correlate information and perform a log review process.

(2) Works with asset custodians to ensure systems are configured to implement automated audit trails for all system components and automatically forward security-related event logs to the SIEM solution to allow [Company Name] security personnel to reconstruct the following events:

a. All individual user accesses to sensitive data (e.g., sensitive data, SSNs, financial accounts, etc.);
b. All actions taken by any individual with root or administrative privileges;
c. Access to all audit trails;
d. Invalid logical access attempts;
e. Use of and changes to identification and authentication mechanisms, including but not limited to:
   i. Creation of new accounts and elevation of privileges; and
   ii. All changes, additions, or deletions to accounts with root or administrative privileges.
f. Initialization, stopping, or pausing of the audit logs; and
g. Creation and deletion of system-level objects.

(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.

Procedures are from the **Cybersecurity Standardized Operating Procedures (CSOP)*

CYBERSECURITY DOCUMENTATION EXAMPLES

Policy | Control Objective | Standard | Guideline | Control | Procedure | **Metric**

METRIC: Metrics are a "point in time" measurement that is designed to facilitate decision making, evaluate performance and improve accountability.

CFG-M-03*

Metric:

- Type: Integer (#)
- Metric: **# platforms with documented baseline configuration standards**
- Calculation: # platforms (e.g., Windows server, Redhat, Cisco IOS, Windows 10, etc.) that have a current, formal baseline configuration that is based on an industry-recognized benchmark (e.g., CIS, DISA STIGs, etc.)

MON-M-05*

Metric:

- Type: Integer (#)
- Metric: **# sources sending logs to the SIEM**
- Calculation: # sources that forward security event logs to the centralized SIEM

MON-M-06*

Metric:

- Type: Integer (#)
- Metric: **# events that become incidents from non-SIEM sources**
- Calculation: # events that escalated into incidents that came from sources other than the SIEM (e.g., personnel reporting to managers, customer feedback, etc.)

Metrics are from the **Digital Security Program (DSP)*

QUESTIONS?

(855) 205-8437 OR SUPPORT@COMPLIANCEFORGE.COM