Version 2023.3

ComplianceForge Reference Model: Hierarchical Cybersecurity Governance Framework (HCGF)

The **ComplianceForge Reference Model** is also referred to as the Hierarchical Cybersecurity Governance Framework (HCGF). This reference model is designed to encourage clear communication by defining cybersecurity and privacy documentation components and how those are linked. This comprehensive view identifies the primary documentation components that are necessary to demonstrate evidence of due diligence and due care. The HCGF addresses the inter-connectivity of policies, control objectives, standards, guidelines, controls, assessment objectives, risks, threats, procedures & metrics. The Secure Controls Framework (SCF) fits into this model by providing the necessary cybersecurity and privacy controls an organization needs to implement to stay both secure and compliant. ComplianceForge simplified the concept of the hierarchical nature of cybersecurity and privacy documentation in the following diagram to demonstrate the unique nature of these components, as well as the dependencies that exist:

Influencers (Internal & External)

Hierarchical cybersecurity governance starts with external influencers – these establish what is considered necessary for due diligence and due care for cybersecurity operations. These include statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding obligations) that organizations must address.

External influencers usually impose meaningful penalties for non-compliance (e.g.., CMMC & NIST 800-171). External influencers are often non-negotiable and are the primary source for defining a need for a policy and provide scoping for control objectives.

Internal influencers focus on management's desire for consistent, efficient and effective operations. This generally takes the form of:
- Business strategy
- Goals & objectives (e.g., customer satisfaction / service levels, budget constraints, quality targets, etc.)

Policies

Policies are high-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes.

Policies are enforced by Standards and further implemented by Procedures to establish actionable and accountable requirements.

Policies are a business decision, not a technical one. Technology determines how policies are implemented. Policies usually exist to satisfy an external requirement (e.g., law, regulation and/or contract).

Control Objectives

Control Objectives are targets or desired conditions to be met. These are statements describing what is to be achieved as a result of the organization implementing a Control.

Control Objectives directly link to laws, regulations and frameworks to align cybersecurity and data privacy with reasonably-expected practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny (e.g., external audits/assessments) to disprove potential accusations of negligence.

Standards

Standards are mandatory requirements in regard to processes, actions, and configurations that are designed to satisfy Controls & Control Objectives.

Standards are intended to be granular and prescriptive to establish **Minimum Security Requirements (MSR)** that ensure systems, applications and processes are designed and operated to include appropriate cybersecurity and data privacy protections.

Guidelines

Guidelines are recommended practices that are based on industry-recognized secure practices. Guidelines help augment Standards when discretion is permissible.

Unlike Standards, Guidelines allow individuals / teams to apply discretion or leeway in interpretation, implementation, or use.

Controls

Controls are technical, administrative or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes.

Controls directly map to Standards, Procedures and Control Objectives. Control testing is designed to measure specific aspects of how Standards are actually implemented and if the Control / Control Objective is sufficiently addressed.

Assessment Objectives (AOs) are a set of determination statements that express the desired outcome for the assessment of a Control. AOs are the authoritative source of guidance for assessing controls to generate evidence to support the assertion that the underlying Control has been satisfied.

Procedures

Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard.

Procedures help address the question of how the organization actually operationalizes a Policy, Standard or Control. Without documented procedures, there will be no defensible evidence of due care practices.

Procedures are generally the responsibility of the process owner / asset custodian to build and maintain, but are expected to include stakeholder oversight to ensure applicable compliance requirements are addressed.

The result of a procedure is intended to satisfy a specific Control. Procedures are also commonly referred to as "control activities."

Risks

Risks represent a situation where someone or something valued is exposed to danger, harm or loss (noun) or to expose someone or something valued to danger, harm or loss (verb).

Risk is often calculated by a formula of the Occurrence Likelihood (OL) x the Impact Effect (IE) in an attempt to quantify the potential magnitude of a risk instance materializing.

In practical terms, a risk is associated with a Control deficiency (e.g., *if the control fails, what risk(s) is the organization exposed to*?)

While it is not possible to have a totally risk-free environment, it may be possible to manage risk by (1) avoiding, (2) reducing, (3) transferring, or (4) accepting risk(s).

An organization should maintain a "risk catalog" that contains organization-specific risks.

Threats

Threats represent a person or thing likely to cause damage or danger (noun) or to indicate impending damage or danger (verb).

In practical terms, a threat is a possible natural or man-made event that affects Control execution. (e.g., *if the threat materializes, will the control function as expected?*)

An organization should maintain a "threat catalog" that contains organization-specific natural and man-made threats that are applicable to its business operations and technologies in use.

Metrics

Metrics provide a "point in time" view of specific, discrete measurements, unlike trending and analytics that are derived by comparing a baseline of two or more measurements taken over a period of time. Analytics are generated from the analysis of metrics.

Analytics are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance-related data.

Good metrics are those that are **SMART** (**S**pecific, **M**easurable, **A**ttainable, **R**epeatable, and **T**ime-dependent)

Internal Influencers

Non-IT related corporate policies
Board of Director (BoD) guidance / directives
Supply Chain Risk Management (SCRM)
Cybersecurity / privacy charter(s)
Other internal requirements

External Influencers - Contractual

CMMC *(CMMC can be both contractual & regulatory)*
PCI DSS
SOC 2 Certification
ISO 27001 Certification
NIST Cybersecurity Framework
Other contractual requirements

External Influencers - Statutory

HIPAA / HITECH
FACTA
GLBA
CCPA
SOX
Data Protection Act (UK)
Other data protection laws

External Influencers - Regulatory

NIST 800-171 / CMMC (FAR & DFARS)
FedRAMP
EU GDPR
Other International Data Protection Laws

CMMC / PCI DSS / NIST CSF / Etc.
CPRA / HIPAA / SOX / Etc.
NIST SP 800-171 / FedRAMP / EU GDPR / Etc.
Policies
Control Objectives
Standards
Guidelines
Assessment Objectives (AOs)
Controls
Procedures
Metrics
Risks
Threats
Every Control Objective Maps To A Policy
Every Standard Maps To A Control Objective
Guidelines Support Applicable Standards
Every Control Maps To A Standard
Every Procedure Maps To A Control
Every Metric Maps To A Control
Every Risk Maps To A Control
Every Threat Maps To A Control
Leading Practices Define Expectations To Be Met (due diligence / due care)
Documents Deviations To Standards
Control Objectives Are Based On Controls
Summarizes Protection Mechanisms
Summarizes Protection Mechanisms
Appropriate Controls Should Be Selected To Meet Specified External & Internal Influencers
Secure Technical Configurations Implement Standards
Summarizes Protection Mechanisms

SUPPORTING COMPLIANCE DOCUMENTATION

Secure Baseline Configurations

A set of specifications for a system, or Configuration Item (**CI**) within a system, application or service, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The secure baseline configuration is used as a basis for future builds, releases, and/or changes.

Risk Register / Plan of Action & Milestones (POA&M)

A POA&M is a document that identifies tasks that need to be accomplished (e.g., a formalized risk register). It details resources required to accomplish the elements of the plan, milestones for meeting the tasks and the scheduled completion dates for the milestones.

System Security Plan (SSP)

A SSP is a document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Top-Down Process Flow of Cybersecurity & Privacy Governance Concepts

Internal & External Influencers primarily drive the development of cybersecurity and privacy policies. This requirements analysis is a component of governance, risk and compliance management practices to appropriately scope security program requirements.

Policies define high-level expectations and provide evidence of due diligence to address applicable requirements (internal and external).

Control Objectives support Policies and provide scoping for Standards, based on industry-recognized secure practices.

Standards operationalize Policies by providing organization-specific requirements that must be met.

Guidelines provide useful guidance that provides additional content to help operationalize Standards.

Controls are assigned to stakeholders to assign responsibilities in enforcing Standards.

Procedures operationalize Standards and Controls. The output of Procedures is evidence of due care to demonstrate that requirements are enforced.

Risks are associated with a control deficiency. (e.g., if the control fails, what risk is the organization exposed to?)

Natural and man-made threats affect control execution (e.g. if the threat materializes, will the control function as expected?)

Metrics provide evidence of an oversight function for the cybersecurity and privacy program by measuring criteria to determine performance.

This document is intended to help standardize cybersecurity and data privacy documentation-related terminology based on definitions from leading authorities (e.g., NIST, ISO, ISACA, AICPA, etc.). In compliance operations, words have meanings. Therefore, it is important to provide examples from industry-recognized sources for the proper use of these terms that make up cybersecurity & data privacy documentation. Simply because an individual has used terminology in a specific manner for past decade (e.g., policy), that does not mean that is correct terminology usage, based on authoritative sources. ComplianceForge took the time to compile authoritative definitions from multiple sources to defend the proper usage that ComplianceForge applies to its documentation structure.

The ComplianceForge Reference Model (**CRM**)[1] is commonly referred to as the Hierarchical Cybersecurity Governance Framework™ (**HCGF**). This reference model is designed to encourage clear communication by clearly defining cybersecurity and data privacy documentation components and how those are linked. This comprehensive view identifies the primary cybersecurity and data privacy documentation components that are necessary to demonstrate evidence of due diligence and due care with applicable laws, regulations and contractual obligations. The HCGF addresses the inter-connectivity of documentation components that is backed by authoritative definitions (as documented in the following pages).

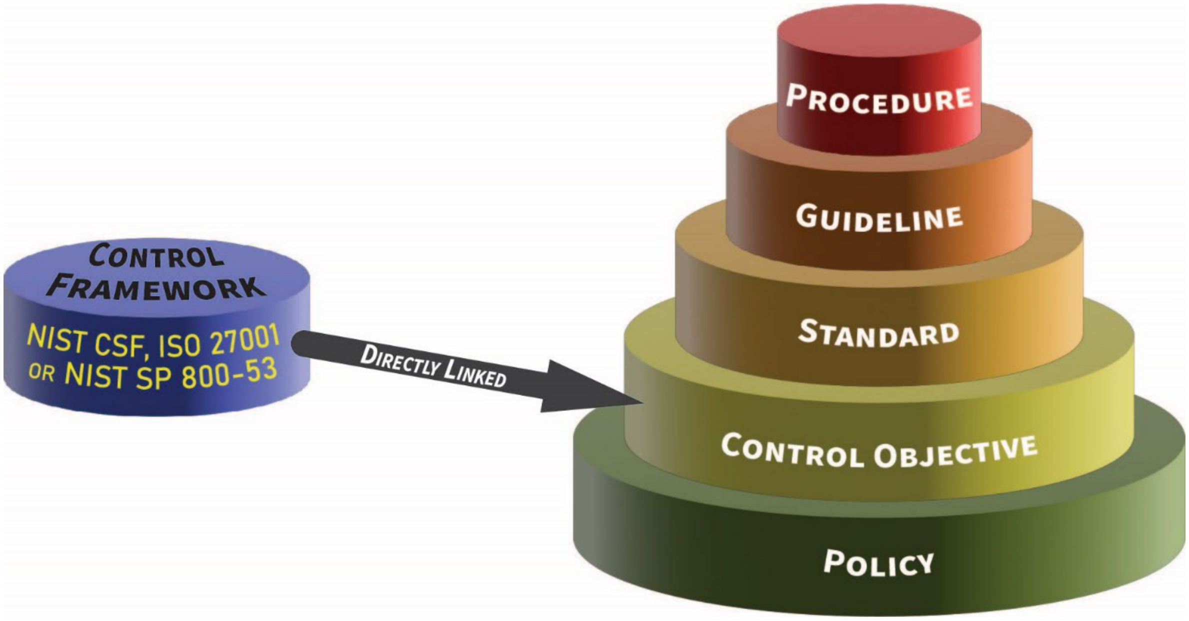
Cybersecurity & Data Privacy Documentation Components

In a business context, cybersecurity and data privacy documentation (e.g., policies, standards, procedures, etc.) provides direction to all employees and contractors within an organization to address applicable needs for secure and compliant practices. This is often dictated by statutory, regulatory and contractual obligations.

Documentation works best when it is simple and concise. Conversely, documentation fails when it is overly wordy, complex or difficult for individuals / teams to find the information they are seeking. When you picture this from a hierarchical perspective, everything builds off the policy and those supporting components also build off each other to make a cohesive and scalable approach to addressing a requirement.

Well-designed cybersecurity & data privacy documentation is comprised of six (6) core components:

(1) Policies that establish 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.



[1] ComplianceForge Reference Model - https://www.complianceforge.com/grc/hierarchical-cybersecurity-governance-framework/

Disclaimer: This document is provided for reference purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a cybersecurity professional.

Policy / Security Policy

Policies are high-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes. Policies are enforced by standards and further implemented by procedures to establish actionable and accountable requirements.

Unfortunately, for many IT/cybersecurity professionals, when they refer to a "policy" they really mean "standard." This common misuse of critical documentation components can create a significant amount of confusion, since those are not interchangeable terms. Standards are subordinate to policies and standards address the granular requirements needed to satisfy a policy. Therefore, a 1-3 sentence policy statement is acceptable to capture a "high-level statement of management intent" for a specific domain.

- It is expected to have multiple policies to address cybersecurity and data privacy needs (e.g., access control, data handling, etc.).
- Policies address the strategic needs of the organization.
- There is never a justifiable reason to have an exception to a policy. Exceptions should only be at the standard or procedure level.

- **ISACA Glossary:**
  - A document that records a high-level principle or course of action that has been decided on.
  - The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams.
  - Overall intention and direction as formally expressed by management.
- **ISO 704:2009:**
  - Any general statement of direction and purpose designed to promote the coordinated planning, practical acquisition, effective development, governance, security practices, or efficient use of information technology resources.
- **ISO 27000:2016:**
  - Intention and direction of an organization as formally expressed by its top management.
- **NIST Glossary (Policy):**
  - Statements, rules or assertions that specify the correct or expected behavior of an entity.
  - A statement of objectives, rules, practices or regulations governing the activities of people within a certain context.
- **NIST Glossary (Security Policy):**
  - Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.
  - A set of rules that governs all aspects of security-relevant system and system element behavior.
    - Note 1: System elements include technology, machine, and human, elements.
    - Note 2: Rules can be stated at very high levels (e.g., an organizational policy defines acceptable behavior of employees in performing their mission/business functions) or at very low levels (e.g., an operating system policy that defines acceptable behavior of executing processes and use of resources by those processes).

Control Objective

Control Objectives are targets or desired conditions to be met. These are statements describing what is to be achieved as a result of the organization implementing a Control, which is what a Standard is intended to address with organization-specific criteria.

Where applicable, Control Objectives are directly linked to laws, regulations and frameworks to align cybersecurity and data privacy with reasonably-expected practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny (e.g., external audits/assessments) to disprove potential accusations of negligence.

- **ISACA Glossary:**
  - A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process.
- **ISO 27000:2016:**
  - Statement describing what is to be achieved as a result of implementing controls.
- **AICPA SSAE No. 18, Attestation Standards Clarification and Recodification:**
  - The aim or purpose of specified controls at the organization. Control objectives address the risks that controls are intended to mitigate.

Disclaimer: This document is provided for reference purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a cybersecurity professional.

Standard

Standards are mandatory requirements regarding processes, actions and configurations that are designed to satisfy Controls and Control Objectives. Standards are intended to be granular and prescriptive to ensure systems, applications and services are designed and operated to include appropriate cybersecurity and data privacy protections.

- **ISACA Glossary:**
  - A mandatory requirement.
- **NIST Glossary:**
  - A published statement on a topic specifying the characteristics, usually measurable, that must be satisfied or achieved to comply with the standard.
  - A rule, condition, or requirement describing the following information for products, systems, services or practices:
    - Classification of components.
    - Specification of materials, performance, or operations; or
    - Delineation of procedures.

Guideline / Supplemental Guidance

Guidelines are recommended practices that are based on industry-recognized secure practices. Guidelines help augment Standards when discretion is permissible. Unlike Standards, Guidelines allow individuals / teams to apply discretion or leeway in interpretation, implementation, or use.

- **ISACA Glossary:**
  - A description of a particular way of accomplishing something that is less prescriptive than a procedure.
- **ISO 704:2009:**
  - Recommendations suggesting, but not requiring, practices that produce similar, but not identical, results.
  - A documented recommendation of how an organization should implement something.
- **NIST Glossary:**
  - Statements used to provide additional explanatory information for security controls or security control enhancements.

Control

Controls are technical, administrative or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes.

Controls directly map to Standards, Procedures and Control Objectives. Control testing is designed to measure specific aspects of how Standards are actually implemented and if the Control / Control Objective is sufficiently addressed.

- **ISACA Glossary:**
  - The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature.
- **ISO 27000:2016:**
  - The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.
  - Measure that is modifying risk:
    - Controls include any process, policy, device, practice, or other actions which modify risk.
    - Controls may not always exert the intended or assumed modifying effect.
- **NIST Glossary:**
  - Measure that is modifying risk. (Note: controls include any process, policy, device, practice, or other actions which modify risk.)
- **NIST SP 800-53 R5:**
  - The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information [security control].
  - The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable data privacy requirements and manage data privacy risks [privacy control].

Disclaimer: This document is provided for reference purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a cybersecurity professional.

Assessment Objective (AO)

Assessment Objectives (AOs) are a set of determination statements that express the desired outcome for the assessment of a Control. AOs are the authoritative source of guidance for assessing Controls to generate evidence that can support an assertion that the underlying Control has been satisfied. Generally, all AOs must be satisfied to legitimately conclude a Control is properly implemented.

- **NIST Glossary:**
  - A set of determination statements that expresses the desired outcome for the assessment of a security control, privacy control, or control enhancement.

Procedure

Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard. Procedures help address the question of how the organization actually operationalizes a Policy, Standard or Control.

Without documented procedures, there can be defendable evidence of due care practices. Procedures are generally the responsibility of the process owner / asset custodian to build and maintain but are expected to include stakeholder oversight to ensure applicable compliance requirements are addressed. The result of a procedure is intended to satisfy a specific control. Procedures are also commonly referred to as “control activities.”

- **ISACA Glossary:**
  - A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.
- **ISO 704:2009:**
  - A detailed description of the steps necessary to perform specific operations in conformance with applicable standards.
  - A group of instructions in a program designed to perform a specific set of operations.
- **NIST Glossary:**
  - A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event.

Threat

Threats represents a person or thing likely to cause damage or danger.

Natural and man-made threats affect control execution (e.g., if the threat materializes, will the control function as expected?). Threats exist in the natural world that can be localized, regional or worldwide (e.g., tornados, earthquakes, solar flares, etc.). Threats can also be man-made (e.g., hacking, riots, theft, terrorism, war, etc.).

- **ISACA Glossary:**
  - Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.
- **ISO 13335-1:**
  - A potential cause of an unwanted incident.
- **NIST Glossary:**
  - Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
  - Cyberthreat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Disclaimer: This document is provided for reference purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a cybersecurity professional.

RISK

Risks represents a potential exposure to danger, harm or loss.*

Risk is associated with a control deficiency (e.g., If the control fails, what risk(s) is the organization exposed to?). Risk is often calculated by a formula of the Occurrence Likelihood (OL) (e.g., probability of the event) x the Impact Effect (IE) (e.g., potential, negative consequences) in an attempt to quantify the potential magnitude of a risk instance materializing.

While it is not possible to have a totally risk-free environment, it may be possible to manage risks by avoiding, reducing, transferring, or accepting the risks.

- **ISACA Glossary:**
  - The combination of the probability of an event and its consequence.
- **ISO 704:2009:**
  - The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- **NIST SP 800-53 R5:**
  - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of:
    - The adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and
    - The likelihood of occurrence.
- **NIST Glossary:**
  - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
    - The adverse impacts that would arise if the circumstance or event occurs; and
    - The likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

* Danger: state of possibly suffering harm or injury
* Harm: material / physical damage
* Loss: destruction, deprivation or inability to use

METRIC

Metrics provide a "point in time" view of specific, discrete measurements, unlike trending and analytics that are derived by comparing a baseline of two or more measurements taken over a period of time.

Analytics are generated from the analysis of metrics. Analytics are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance related metrics.

- **ISACA Glossary:**
  - A quantifiable entity that allows the measurement of the achievement of a process goal.
- **ISO 704:2009:**
  - A thing that is measured and reported to help with the management of processes, services, or activities.
- **NIST Glossary:**
  - Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

Disclaimer: This document is provided for reference purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a cybersecurity professional.

Secure Baseline Configurations / Hardening Standard

Secure baseline configurations (e.g., hardening standard) are technical in nature and specify the required configuration settings for a defined technology platform.

Leading guidance on secure configurations tend to come from:

- Center for Internet Security (CIS) Benchmarks;
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs); and/or
- Original Equipment Manufacturer (OEM) recommendations.

- NIST Glossary:
  - A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
  - A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Risk Register / Plan of Action & Milestones (POA&M)

A POA&M is a "living document" that summarizes control deficiencies from identification through remediation. A POA&M is essentially a risk register that tracks the assignment of remediation efforts to individuals or teams, as well as identifying the tasks and resources necessary to perform the remediation.

- NIST Glossary:
  - Risk Register: A repository of risk information including the data understood about risks over time.
  - Risk Register: A central record of current risks, and related information, for a given scope or organization. Current risks are comprised of both accepted risks and risk that are have a planned mitigation path (e.g., risks to-be-eliminated as annotated in a POA&M).
  - POA&M: A document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones.

System Security Plan (SSP) / System Security & Privacy Plan (SSPP)

A SSP/SSPP is a "living document" that summarizes protection mechanisms for a system or project. It is a documentation method used to capture pertinent information in a condensed manner so that personnel can be quickly educated on the "who, what, when, where, how & why" concepts pertaining to the security of the system or project. A SSP/SSPP is meant to reference an organization's existing policies, standards and procedures and is not a substitute for that documentation.

- NIST Glossary:
  - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Disclaimer: This document is provided for reference purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a cybersecurity professional.