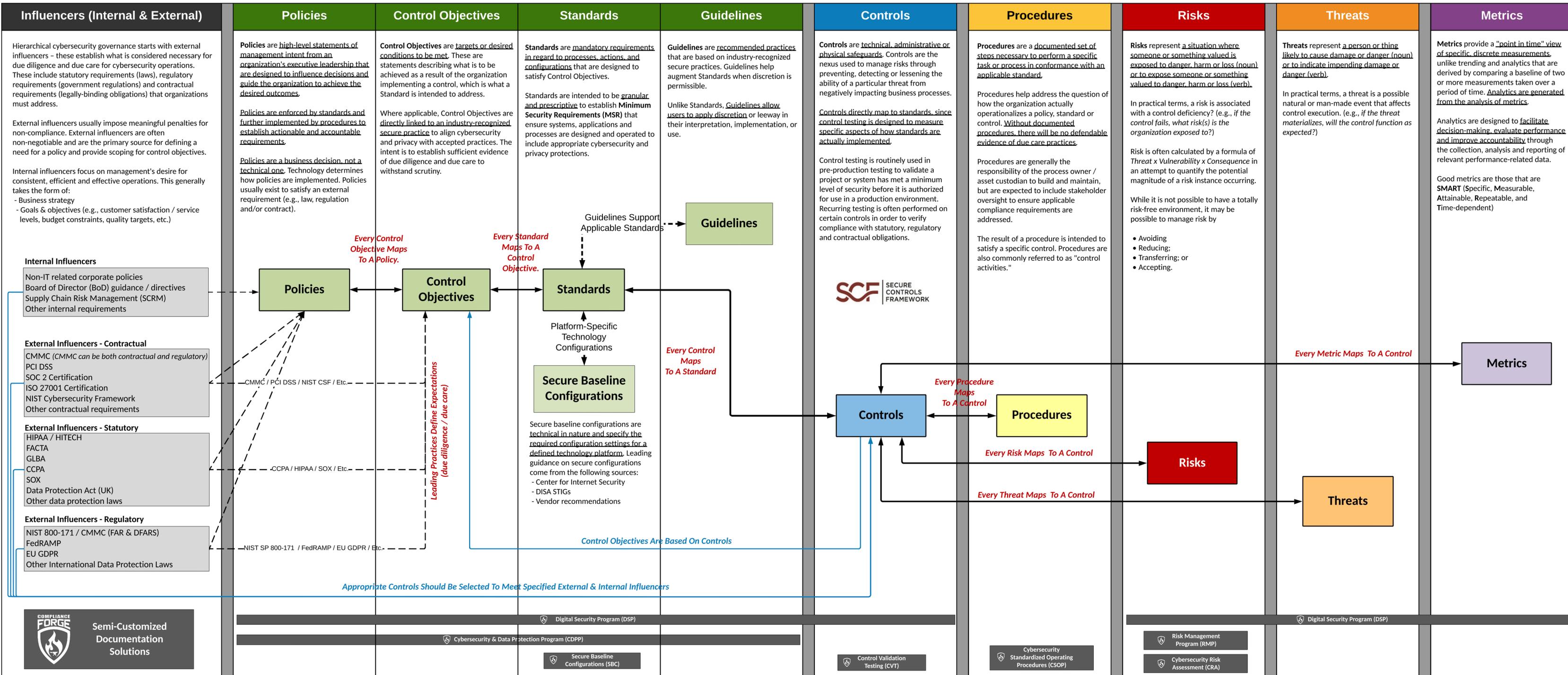


The **ComplianceForge Reference Model** is commonly referred to as the **Hierarchical Cybersecurity Governance Framework™ (HCGF)**. This reference model is designed to encourage clear communication by clearly defining cybersecurity and privacy documentation components and how those are linked. This comprehensive 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, risks, 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 has 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:



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.

## COMPLIANCEFORGE REFERENCE MODEL: DEFINING DOCUMENTATION COMPONENT TERMINOLOGY

Since words have meanings, it is important to provide examples from industry-recognized sources for the proper use of these terms that make up cybersecurity & privacy documentation. The ComplianceForge Reference Model is designed to encourage clear communication by clearly 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. This reference model addresses the inter-connectivity of policies, control objectives, standards, guidelines, controls, risks, procedures & metrics.

### 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. 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).

- **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. Where applicable, Control Objectives are directly linked to an industry-recognized secure practice to align cybersecurity and privacy with accepted practices. The intent is to establish sufficient evidence of due diligence and due care to withstand scrutiny.

- **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.

## STANDARD

Standards are mandatory requirements regarding processes, actions and configurations that are designed to satisfy Control Objectives. Standards are intended to be granular and prescriptive to ensure systems, applications and processes are designed and operated to include appropriate cybersecurity and 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 users to apply discretion or leeway in their 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, since control testing is designed to measure specific aspects of how standards are actually implemented.

- **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 privacy requirements and manage privacy risks [privacy control].

## 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 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.”

- **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.

## 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 Threat x Vulnerability x Consequence in an attempt to quantify the potential magnitude of a risk instance occurring. 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

## THREAT

Threats represent 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 manmade (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.

## 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 data. Good metrics are those that are SMART (Specific, Measurable, Attainable, Repeatable, and Time-dependent)

- **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.