Understanding The Hierarchical Nature of Cybersecurity & Privacy Documentation

version 2020.2

The **ComplianceForge** Hierarchical Cybersecurity Governance Framework™ (HCGF) takes a comprehensive view towards the necessary documentation components that are key to being able to demonstrate evidence of due diligence and due care. This framework addresses the interconnectivity 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:

COMPLIANCE FORGE

HIERARCHICAL CYBERSECURITY GOVERNANCE FRAMEWORK™ - INTERCONNECTIVITY OF POLICIES, CONTROL OBJECTIVES, STANDARDS, GUIDELINES, CONTROLS, RISKS, PROCEDURES & METRICS

INFLUENCERS (EXTERNAL & INTERNAL)

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. 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.)

Internal Influencers
- Non-IT related corporate policies
- Board of Director (BoD) guidance / directives
- Other internal requirements

External Influencers - Contractual
- CMMC
- PCI DSS
- SOC 2
- ISO 27001
- 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 (FAR & DFARS)
- FedRAMP
- EU GDPR
- Other International Data Protection Laws

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, 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.

STANDARDS

Standards are mandatory requirements in regard to processes, actions, and configurations that are designed to satisfy 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 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 users to apply discretion or leeway in their 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, since control testing is designed to measure specific aspects of how standards are actually implemented.

Control testing is routinely used in pre-production testing to validate a project or system has met a minimum level of security before it is authorized for use in a production environment. Recurring testing is often performed on certain controls in order to verify compliance with statutory, regulatory and contractual obligations.

RISKS

Risks represents a potential exposure to harm or loss. 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.

Questionnaires are often used to determine if a control is met. While this is often a YES / NO option, approach is often fallible and does not provide proper insight into most risk. Assessing controls against a targeted level of process maturity provides a more accurate insight into existing risks, specific to the control in question.

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 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."

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)

Policies

Control Objectives

Standards

Guidelines

Controls

Control Questions

Procedures

Metrics

Secure Baseline Configurations

Every Control Objective Maps To A Policy.

Every Standard Maps To A Control Objective.

Guidelines Support Applicable Standards

Platform-Specific Technology Configurations

Every Control Maps To A Standard

Every Risk Maps To A Control

Every Metric Maps To A Control

Every Procedure Maps To A Control

Leading Practices Define Expectations For Due Care Expectations

CMMC / PCI DSS / NIST CSF / Etc.

CCPA / HIPAA / SOX / Etc.

NIST 800-171 / FedRAMP / EU GDPR / Etc.

Secure baseline configurations are technical in nature and specify the required configuration settings for a defined technology platform. Leading guidance on secure configurations come from the following sources:
- Center for Internet Security
- DISA STIGs
- Vendor recommendations

SCF SECURE CONTROLS FRAMEWORK

Digital Security Program (DSP)

Written Information Security Program (WISP)

Secure Baseline Configurations (SBC)

Control Validation Testing (CVT)

Cybersecurity Standardized Operating Procedures (CSOP)

Digital Security Program (DSP)

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.

Structuring controls as questions is often used to in questionnaire format to evaluate the implementation of a control.

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

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