Policy vs Standard vs Control vs Procedure

Cybersecurity, IT professionals and legal professionals routinely abuse the terms “policy” and “standard” as if these words were synonymous. In reality, these terms have quite different implications, and those differences should be kept in mind since the use of improper terminology has cascading effects that can negatively impact the internal controls of an organization. The information below is meant to help get everyone on the same sheet of music, since words do have meanings and it is important to understand cybersecurity and privacy requirements. In the context of good cybersecurity & privacy documentation, policies and standards are key components that are intended to be hierarchical and build on each other to build a strong governance structure that utilizes an integrated approach to managing requirements.

A common question is “What is the difference between a policy vs a standard?”

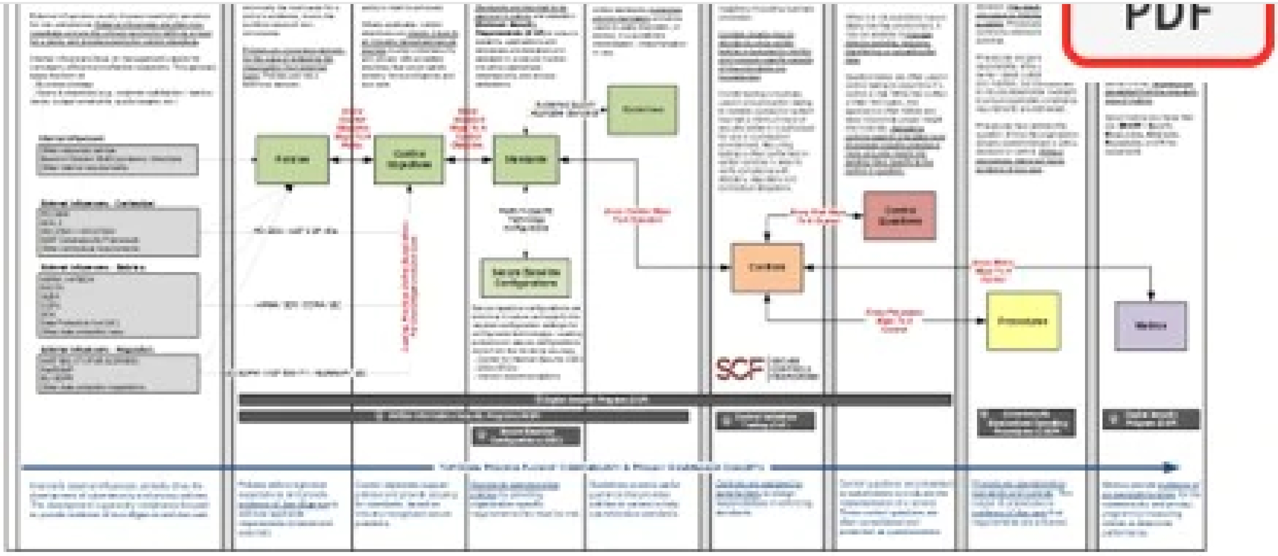
In simple terms, a policy is a high-level statement of management intent that formally establishes requirements to guide decisions and achieve rational outcomes. A policy is intended to come from the CEO or board of directors that has strategic implications. However, a standard is a formally-established requirement in regard to a process, action or configuration that is meant to be an objective, quantifiable expectation to be met (e.g., 8 character password, change passwords every 90 days, etc.).

In reality, no one should ever ask for an exception to a policy. Exceptions should only be for standards when there is a legitimate business reason or technical limitation that precludes a standard from being followed (e.g., vulnerability scanning exception for a "fragile" application that breaks when scanned by the default scanning profile). It is important that if a standard is granted an exception, there should be a compensating control placed to reduce that increased risk from the lack of the required standard (e.g., segment off the application that cannot be scanned for vulnerabilities).

Documentation Should Be Hierarchical: Policy > Standard

In an effort to help clarify this concept, 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 downloadable diagram to demonstrate the unique nature of these components, as well as the dependencies that exist:

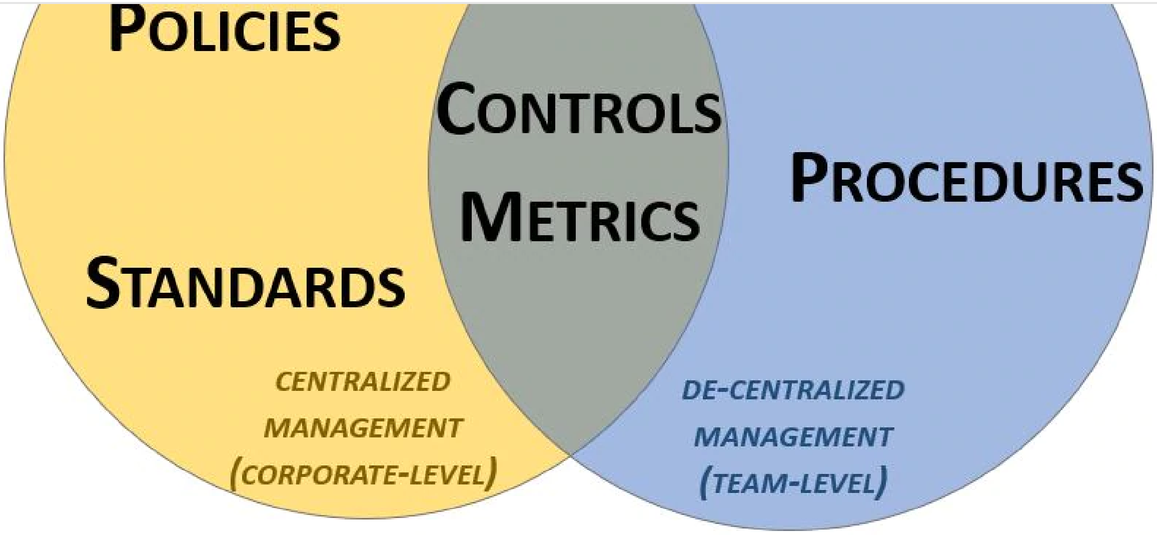


One of the most important things to keep in mind with procedures is that the "ownership" is different than that of policies and standards:

- Policies, standards and controls are designed to be centrally-managed at the corporate level (e.g., governance, risk & compliance team, CISO, etc.)
- Controls are assigned to stakeholders, based on applicable statutory, regulatory and contractual obligations
- Procedures are by their very nature de-centralized, where control implementation at the control level is defined to explain how the control is addressed.

Given this approach to how documentation is structured, based on "ownership" of the documentation components:

- Policies, standards and controls are expected to be published for anyone within the organization to have access to, since it applies organization-wide. This may be centrally-managed by a GRC/IRM platform or published as a PDF on a file share, since they are relatively static with infrequent changes.
- Procedures are "living documents" that require frequent updates based on changes to technologies and staffing. Procedures are often documented in "team share" repositories, such as a wiki, SharePoint page, workflow management tool, etc.



Why Should You Care?

Governance is built on words. Beyond just using terminology properly, understanding the meaning of these concepts is crucial in being able to properly implement cybersecurity and privacy governance within an organization. An indicator of a well-run governance program is the implementation of hierarchical documentation since it involves bringing together the right individuals to provide appropriate direction based on the scope of their job function.

To help visualize that concept, imagine the board of directors of your organization publishing procedural process guidance for how a security analyst performs daily log review activities. Most would agree that such a scenario is absurd since the board of directors should be focused on the strategic direction of the company and not day-to-day procedures.

However, in many organizations, the inverse occurs where the task of publishing the entire range of cybersecurity documentation is delegated down to individuals who might be competent technicians but do not have insights into the strategic direction of the organization. This is where the concept of hierarchical documentation is vitally important since there are strategic, operational, and tactical documentation components that have to be addressed to support governance functions.

Understanding the hierarchy of cybersecurity documentation can lead to well-informed risk decisions, which influence technology purchases, staffing resources, and management involvement. That is why it serves both cybersecurity and IT professionals well to understand the cybersecurity governance landscape for their benefit, as it is relatively easy to present issues of non-compliance in a compelling business context to get the resources you need to do your job.

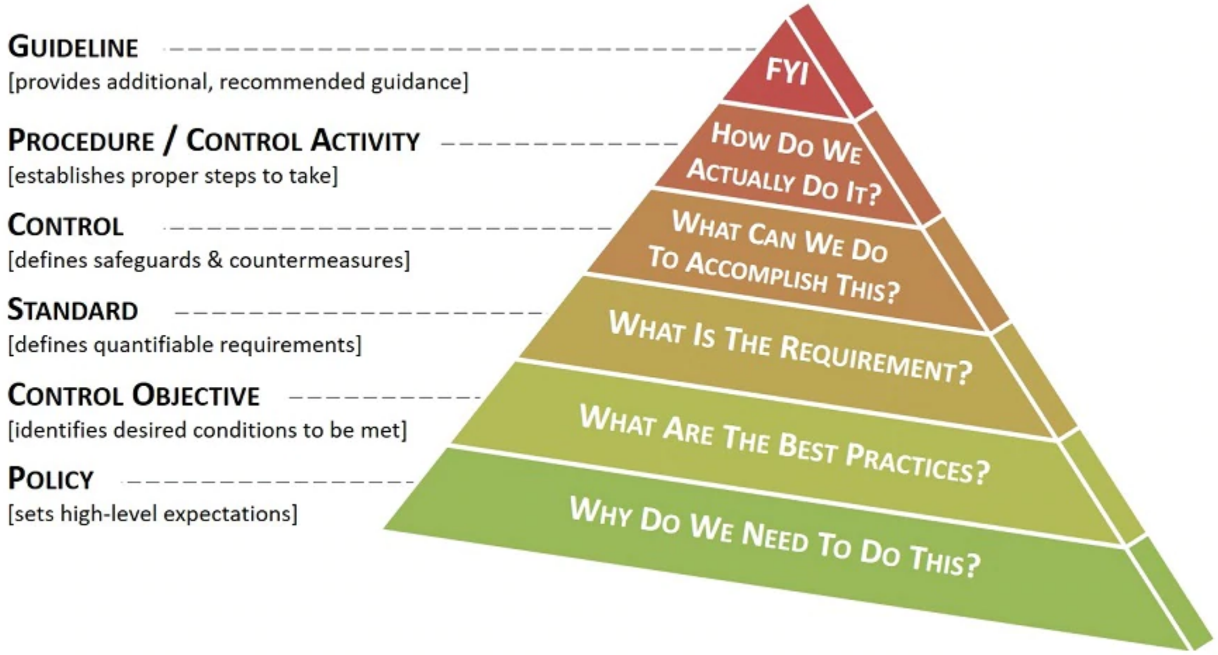
What Wrong Looks Like

architected documentation include:

- Human nature is always the mortal enemy of unclear documentation, as people will not take the time to read it. An ignorant or ill-informed workforce entirely defeats the premise of having the documentation in the first place.
- If the goal is to be "audit ready" with documentation, having excessively-wordy documentation is misguided. Excessive prose that explains concepts *ad nauseum* in paragraph after paragraph makes it very hard to understand the exact requirements, and that can lead to gaps in compliance.

What Right Looks Like

In the context of good cybersecurity documentation, these components are hierarchical and build on each other to build a strong governance structure that utilizes an integrated approach to managing requirements.


GUIDELINE
[provides additional, recommended guidance]
PROCEDURE / CONTROL ACTIVITY
[establishes proper steps to take]
CONTROL
[defines safeguards & countermeasures]
STANDARD
[defines quantifiable requirements]
CONTROL OBJECTIVE
[identifies desired conditions to be met]
POLICY
[sets high-level expectations]
FYI
HOW DO WE ACTUALLY DO IT?
WHAT CAN WE DO TO ACCOMPLISH THIS?
WHAT IS THE REQUIREMENT?
WHAT ARE THE BEST PRACTICES?
WHY DO WE NEED TO DO THIS?

A picture is sometimes worth 1,000 words – this concept can be seen here in a swim lane diagram.

Policy.

- A policy is a high-level statement of management intent that formally establishes requirements to guide decisions and achieve rational outcomes.
- Essentially, a policy is a statement of expectation, that is enforced by standards and further implemented by procedures.
- External influencers, such as statutory, regulatory, or contractual obligations, are commonly the root cause for a policy's existence.

Where applicable, Control Objectives should be directly linked to an industry-recognized practice (e.g., statutory, regulatory or contractual requirements).

Standard.

Standards are formally-established requirements in regard to processes, actions, and configurations.

Standards are finite, quantifiable requirements that satisfy Control Objectives.

Exceptions are always to Standards and never to Policies. If a standard cannot be met, it is generally necessary to implement a compensating control to mitigate the risk associated with that deficiency.

Control.

Unlike Standards, Controls define the actual safeguards and countermeasures that are assigned to a stakeholder (e.g., an individual or team) to implement.

Controls testing is designed to monitor and measure specific aspects of a Standard to ensure a Standard is properly implemented.

Controls are the technical, administrative or physical safeguards that exist to prevent, detect or lessen the ability of a threat to exploit a vulnerability.

Procedure.

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

Procedures are the responsibility of the asset custodian to build and maintain in support of standards and policies.

Guideline.

Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Guidelines are generally recommended practices that are based on industry-recognized practices or cultural norms within an organization.

Guidelines help augment Standards when discretion is permissible.

Questions? Please contact us for clarification so that we can help you find the right solution for your cybersecurity and privacy compliance needs.

Find Out Exclusive Information On Cybersecurity

COMPLIANCE FORGE

Search Compliance Forge

NY Education Law 2-D - NIST CSF Compliance

For school districts in New York state, the NY education law 2-D is compelling school districts to c...

Texas SB 820 - New Law Requires Cybersecurity Policies for Texas School Districts

Texas SB 820 goes into effect on 1 September 2019 that requires every school district in Texas to ad...

VISIT OUR FAQS

Questions about our products?

More Info

CUSTOMER SERVICE

Our customer service is here to help you get answers quickly!

More Info

WHY CYBERSECURITY

Find out the importance of these documents for your business.

More Info

BLOG

Read exclusive information about cybersecurity from Compliance Forge.

More Info

30 N Gould St
Suite 9141
Sheridan, WY 82801

Newsletter Sign Up

First Name

Email Address

Sign Up Now

Search Compliance Forge

Errata
FAQ
Partners
Reasons To Buy
Blog
Sitemap

My Account
About Us
Terms & Conditions
Privacy
Customer Service

Veteran-Owned Small Business (VOSB) | DUNS: 080724402 | CAGE Code: 7XAZ4 | NAICS Codes: 541690, 541519, & 541611

This website does not render professional services advice and is not a substitute for dedicated professional services. If you have compliance questions, you should consult a cybersecurity or privacy professional to discuss your specific needs. Compliance Forge, LLC (ComplianceForge) disclaims any liability whatsoever for any documentation, information, or other material which is or may become a part of the website. ComplianceForge does not warrant or guarantee that the information will not be offensive to any user. User is hereby put on notice that by accessing and using the website, user assumes the risk that the information and documentation contained in the web site may be offensive and/or may not meet the needs and requirements of the user. The entire risk as to the use of this website is assumed by the user.

ComplianceForge reserves the right to refuse service, in accordance with applicable statutory and regulatory parameters.