# START HERE:

## A GUIDE TO UNDERSTANDING CYBERSECURITY & DATA PRIVACY DOCUMENTATION

version 2024.1

## Table of Contents

## Understanding The Documentation Side of Cybersecurity & Data Privacy

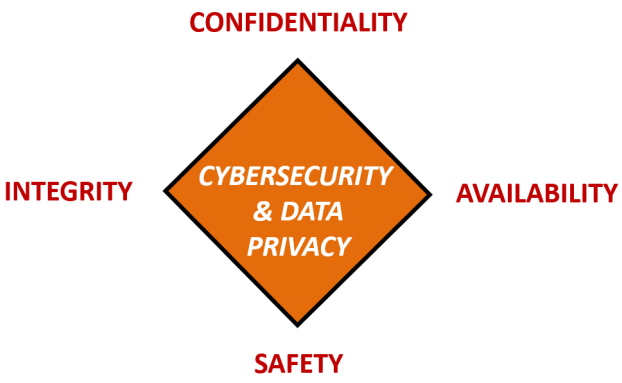
Thank you for taking the time to read this document, since it is intended to help establish a baseline understanding of "industry-recognized practices" around cybersecurity & data privacy documentation. If you are reading this, it is a good indication that your company is committed to protecting itself, as well as its employees, partners, and clients from damaging acts that are intentional or unintentional.

Effective cybersecurity & data privacy is a team effort involving the participation and support of every user that interacts with your company's data and/or systems, it is a necessity for your company's cybersecurity & data privacy requirements to be made available to all users in a format that they can understand. That means your company must publish those requirements in some manner, generally in either PDF format or published to an internal source (e.g., wiki, SharePoint, Jira, GRC, etc.). Our goal is to make that process as efficient, cost-effective and scalable, as possible.

If you have any questions, please reach out to us at support@complianceforge.com or 1-855-205-8437.

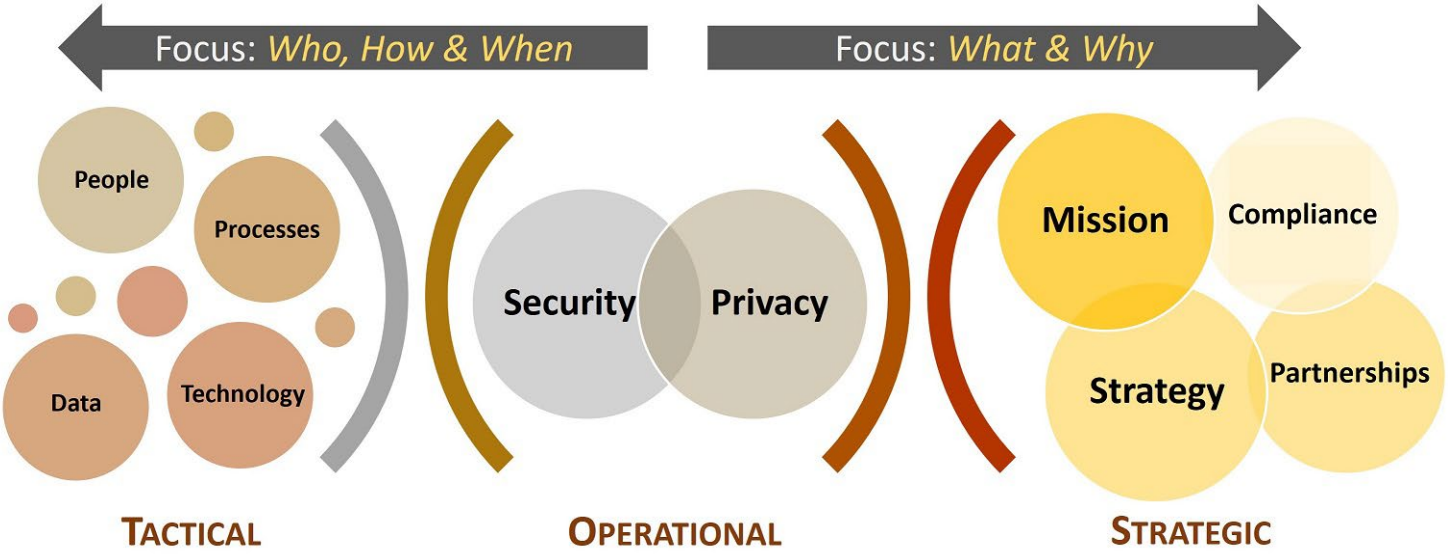
### Addresses The Four-Pillars of Cybersecurity & Data Privacy

Protecting the data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, security and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:




- **Confidentiality** – This addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal privacy and proprietary information.
- **Integrity** – This addresses protecting against improper modification or destruction, including ensuring non-repudiation and authenticity.
- **Availability** – This addresses timely, reliable access to data, systems and services for authorized users, services and processes.
- **Safety** – This addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

Your cybersecurity & data privacy documentation is meant to address the "who, what, when, how & why" across the strategic, operational and tactical needs of your organization:



## What Cybersecurity & Data Privacy Documentation Looks Like When It Is Done Right

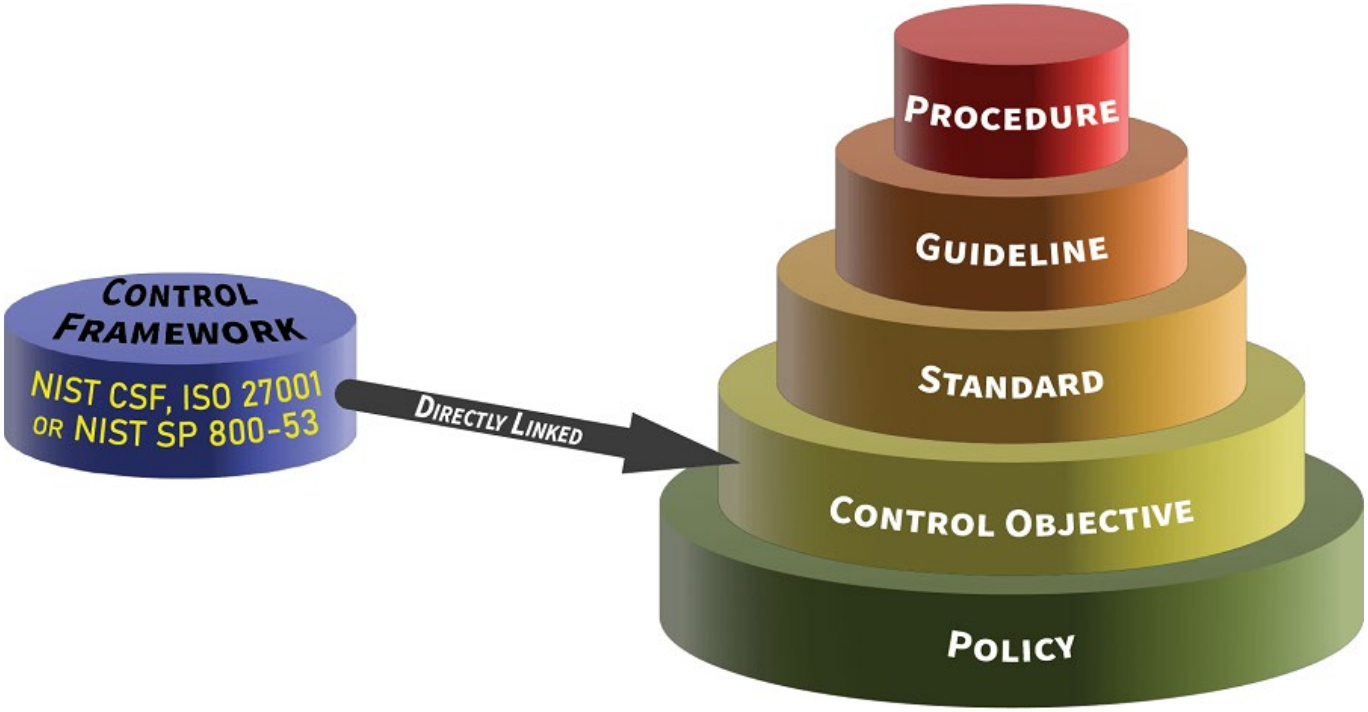
In a business context, cybersecurity & data privacy documentation (e.g., policies, standards, procedures, etc.) provide direction to all employees and contractors within a company to address needs for secure practices. This guidance for cybersecurity & data privacy is intended to be in accordance with the company's business objectives, as well as relevant laws and other legal obligations for cybersecurity & data privacy.

### Cybersecurity Documentation Components

Documentation works best when it is simple and concise. Conversely, documentation fails when it is overly wordy, complex or difficult for users 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 documentation is generally comprised of six (6) main parts:

1. Policies establish management's intent;
2. Control Objectives identify leading practices (mapped to requirements from laws, regulations and frameworks);
3. Standards provide quantifiable requirements;
4. Controls identify desired conditions that are expected to be met (requirements from laws, regulations and frameworks);
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.




### Understanding The Purpose of Cybersecurity Documentation

The purpose of a company's cybersecurity & data privacy documentation is to prescribe a comprehensive framework for:

- Creating a clearly articulated approach to how your company handles cybersecurity – in terms of ISO 27001, this concept would be considered an Information Security Management System (**ISMS**).
- Protecting the confidentiality, integrity, availability and safety of data and systems on your network.
- Providing guidance to help ensure the effectiveness of cybersecurity & data privacy controls that are put in place to support your company's operations.
- Helping your users to recognize the highly-networked nature of the current computing environment to provide effective company-wide management and oversight of those related cybersecurity risks.

The objective is to provide management direction and support for cybersecurity & data privacy in accordance with business requirements and relevant laws and regulations.

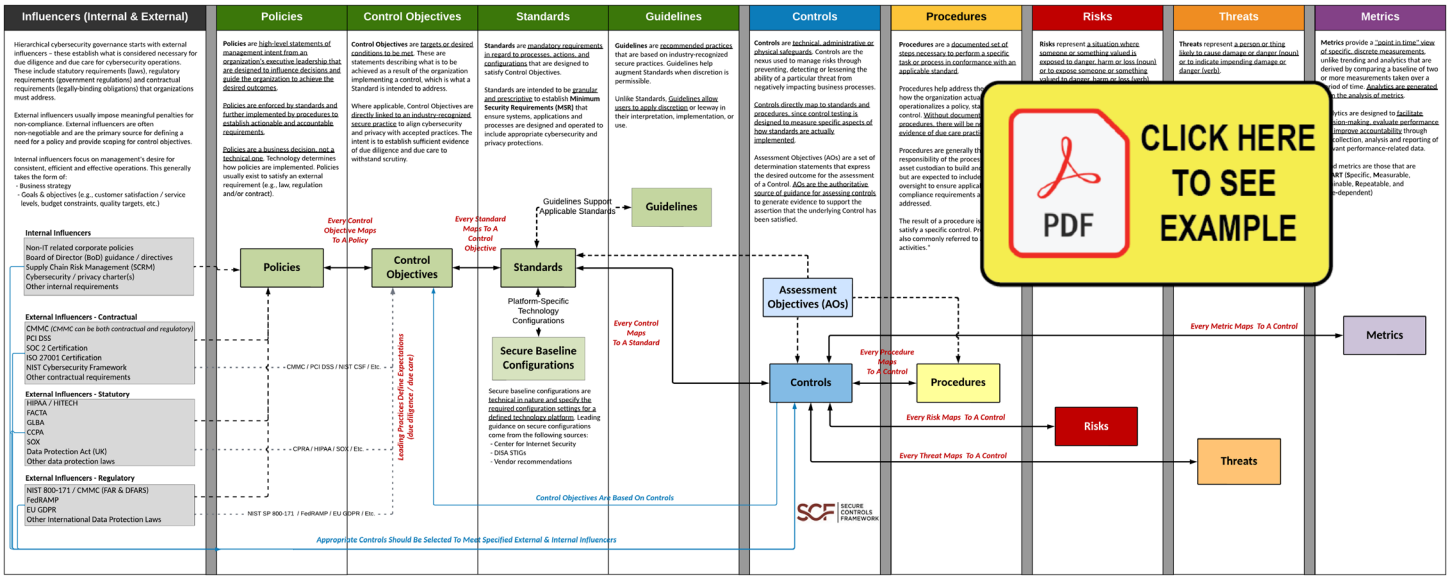
## Cybersecurity Documentation Hierarchy – Understanding How Cybersecurity & Data Privacy Documentation Is Connected

It all starts with influencers – these influencers set the tone and establish what is considered to be due care for cybersecurity & data privacy operations. For external influencers, this includes statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding agreements) that companies must address. For internal influencers, these are business-driven and the focus is more on management's desire for consistent, efficient and effective operations:

- Alignment with business strategy
- Meeting business goals & objectives

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).

When that is all laid out properly, your company's cybersecurity & data privacy documentation should be hierarchical and linked from policies all the way through metrics (as shown in the diagram below).




**Downloadable graphic at: https://content.complianceforge.com/Hierarchical-Cybersecurity-Governance-Framework.pdf**

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

# PUT AN END TO "WORD CRIMES" – UNDERSTANDING DOCUMENTATION COMPONENT TERMINOLOGY

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.

## 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.

## 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].

## 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 is no 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.

## 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.

## 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.

## Not Sure Which Cybersecurity Framework Your Company Needs?

When it really comes down to it, there are only a few frameworks for cybersecurity that are commonly-accepted as "best practices" and those are listed below:

- NIST Cybersecurity Framework (**NIST CSF**)
- ISO 27001/27002
- NIST SP 800-53
- Secure Controls Framework (**SCF**)


### Aligning With A Framework Is More Than Just Policies, Standards & Procedures

To do NIST CSF, ISO 27002 or NIST SP 800-53 properly, it takes more than just a set of policies and standards. While those are foundational to building a cybersecurity program aligned with that framework, there is a need for program-specific guidance that helps operationalize those policies and standards (e.g., risk management program, third-party management, vulnerability management, etc.). It is important to understand what is required to comply with NIST CSF vs ISO 27002 vs NIST SP 800-53, since there are significantly different levels of expectation.

It is important to understand that picking a cybersecurity framework is more of a business decision and less of a technical decision. Realistically, the process of selecting a cybersecurity framework must be driven by a fundamental understanding of what your organization needs to comply with from a statutory, regulatory and contractual perspective, since that understanding establishes the minimum set of requirements necessary to:

(1) Not be considered negligent with reasonable expectations for cybersecurity & Data Privacy;
(2) Comply with applicable laws, regulations and contractual obligations; and
(3) Implement the proper controls to secure your systems, applications and processes from reasonable threats, based on your specific business case and industry practices.

This understanding makes it easy to determine where on the "framework spectrum" (shown above) you need to focus for selecting a set of cybersecurity principles to follow. This process generally leads to selecting either the NIST Cybersecurity Framework, ISO 27002 or NIST SP 800-53 as a starting point.

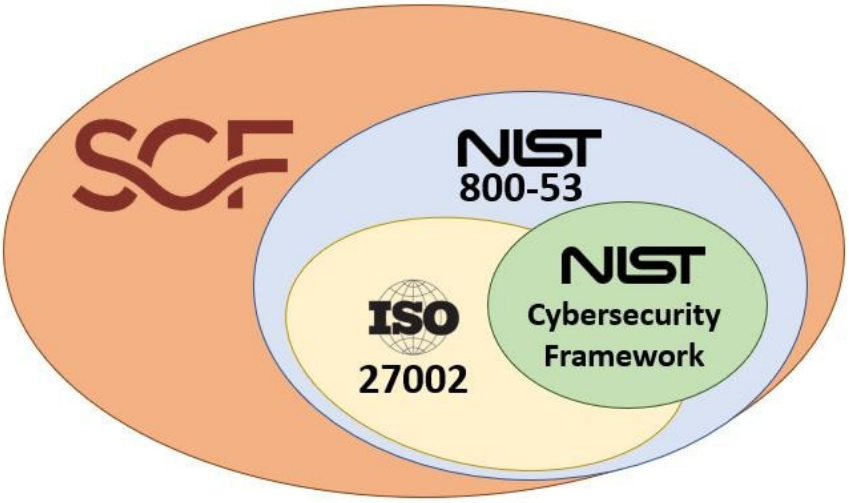
A key consideration for picking a cybersecurity framework involved understanding the level of content each framework offers, since this directly impacts the available security and privacy controls that exist "out of the box" without having to bolt-on content to make it work for your specific needs. If you ask a cybersecurity professional to identify their preferred "best practice framework", it generally comes down to NIST or ISO. If you look at this from the perspective of a debate over which soft drink tastes best (e.g., **Coke vs Pepsi**), it generally comes down to personal preferences, since both products are essentially sugary, carbonated drinks and only differ slightly in flavor and packaging. The same arguments can be made for cybersecurity's two heavy hitters – NIST SP 800-53 and ISO 27002. Gaining popularity is the NIST Cybersecurity Framework (NIST CSF), but it lacks appropriate coverage out of the box to be considered a comprehensive cybersecurity framework. On the robust side is the SCF that is a metaframework that covers them all.

## NIST CSF < ISO 27002 < NIST SP 800-53 < Secure Controls Framework

To help visualize it, ISO 27002 is essentially a subset of NIST SP 800-53 where the fourteen (14) sections of ISO 27002 security controls fit within the twenty (20) families of NIST SP 800-53 rev5 security controls. The NIST CSF is a subset of NIST SP 800-53 and also shares controls found in ISO 27002. The NIST CSF takes parts of ISO 27002 and parts of NIST SP 800-53, but is not inclusive of both. That makes the NIST CSF a decent choice for smaller companies that need a set of "best practices" to align with, where ISO 27002 and NIST SP 800-53 are better for larger companies or those that have unique compliance requirements.

Unfortunately, common requirements such as the Payment Card Industry Data Security Standard (PCI DSS) are more comprehensive than what is included natively by NIST CSF, so you would need to use ISO 27002 or NIST SP 800-53 to meet PCI DSS as a framework, unless you want to bolt-on additional controls to the NIST CSF to make that work. Is that wrong? No, but it is just messy when you start bolting onto frameworks. Think of "bolting on" to frameworks along the lines of gnawing off the square sides of a peg to make it fit into a round hole, where it will eventually fit but it likely will not look very good.

The SCF is a "metaframework" which is a framework of frameworks. The SCF is a superset that covers the controls found in NIST CSF, ISO 27002, NIST SP 800-53 and over 100 other laws, regulations and frameworks. These leading cybersecurity frameworks tend to cover the same fundamental building blocks of a cybersecurity program, but differ in some content and layout. Before picking a framework, it is important to understand that each one has its benefits and drawbacks. Therefore, your choice should be driven by the type of industry your business is in and what laws, regulations and contractual obligations your organization needs to comply with.




### Secure Controls Framework (SCF) Overview

If you are not familiar with the Secure Controls Framework (SCF), it was developed with the ambitious goal of providing a comprehensive catalog of cybersecurity & data privacy control guidance to cover the strategic, operational and tactical needs of organizations, regardless of its size, industry or country of origin. By using the SCF, your IT, cybersecurity, legal and project teams can speak the same language about controls and requirement expectations!

The SCF is an open source project that provides free cybersecurity & data privacy controls for business. The SCF focuses on internal controls, which are the cybersecurity & data privacy-related policies, standards, procedures and other processes that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected.

The SCF is a "best in class" approach that covers NIST SP 800-53, ISO 27002, NIST CSF and many other frameworks. Being a hybrid, it allows you to address multiple cybersecurity & data privacy frameworks simultaneously. The SCF is a free resource for businesses to use. ComplianceForge's Digital Security Program (DSP) has 1-1 mapping with the SCF, so the DSP provides the most comprehensive coverage of any ComplianceForge product.

## NIST SP 800-53 Overview

The National Institute of Standards and Technology (NIST) is on the fifth revision (rev5) of Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53 has become the de facto standard for private businesses that do business with the US federal government.

One thing to keep in mind is that NIST SP 800-53 is a super-set of ISO 27002 - that means you will find all the components of ISO 27002 covered by NIST SP 800-53. However, ISO 27002 does not cover all of the areas of NIST SP 800-53.

The Federal Information Security Management Act (FISMA) and the Department of Defense Information Assurance Risk Management Framework (RMF) rely on the NIST SP 800-53 framework, so vendors to the US federal government must meet those same requirements in order to pass these rigorous certification programs. Additionally, for NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST SP 800-53 is called out as the best practices for government contractors to secure their systems. That further helps strengthen NIST SP 800-53 as a best practice within the US, especially for any government contractors.

NIST SP 800-53 includes what both ISO 27002 and NIST CSF addresses, as well as a whole host of other requirements. NIST SP 800-53 is the basis for the controls found in NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC). NIST SP 800-53 is commonly found in the financial, medical and government contracting industries. One great thing about NIST SP 800-53, and it applies to all NIST publications, is that it is freely available, at no cost to the public - http://csrc.nist.gov/publications/PubsSPs.html.

## ISO 27002 Overview

The International Organization for Standardization (ISO) is a non-governmental organization that is headquartered in Switzerland. ISO can be a little more confusing for newcomers to IT security or compliance, since a rebranding occurred in 2007 to keep ISO's IT security documents in the 27000 series of their documentation catalog - ISO 17799 was renamed and became ISO 27002. To add to any possible confusion, ISO 27002 is a supporting document that aids in the implementation of ISO 27001. Adding a little more confusion to the mix, it is important to note that companies cannot certify against ISO 27002, just ISO 27001. ISO 27001 Appendix A contains the basic overview of the security controls needed to build an Information Security Management System (ISMS), but ISO 27002 provides those specific controls that are necessary to actually implement ISO 27001. Essentially, you can't meet ISO 27001 without implementing ISO 27002.

To keep things simple, just remember that ISO 27001 lays out the framework to create an "Information Security Management System" (e.g., a comprehensive IT security program), whereas ISO 27002 contains the actual "best practices" details of what goes into building a comprehensive IT security program. Since ISO's information security framework has been around since the mid-1990s, it was in "right time at the right place" to evolve into the de facto IT security framework outside of the United States. You will find ISO 27002 extensively used by multinational corporations and for companies that do not have to specifically comply with US federal regulations. ISO 27002 is also "less paranoid" than NIST SP 800-53, which has an advantage of being less complex and therefore easier implement.

ISO 27002 is an internationally-recognized cybersecurity framework that provides coverage for many common requirements (e.g., PCI DSS, HIPAA, etc.). One unfortunate thing about ISO 27002, and it applies to all ISO publications, is that ISO charges for its publications - http://www.iso.org/iso/home/store.htm.

## NIST Cybersecurity Framework Overview

The NIST Cybersecurity Framework (NIST CSF) does not introduce new standards or concepts, but leverages and integrates industry-leading cybersecurity practices that have been developed by organizations like NIST and ISO. The CSF comprises a risk-based compilation of guidelines that can help organizations identify, implement, and improve cybersecurity practices, and creates a common language for internal and external communication of cybersecurity issues. The NIST CSF is designed to evolve with changes in cybersecurity threats, processes, and technologies. Essentially, the NIST CSF envisions effective cybersecurity as a dynamic, continuous loop of response to both threats and solutions.

The downside to the NIST CSF is that its brevity makes it incompatible with common compliance requirements, such as NIST SP 800-171, PCI DSS, and HIPAA. For those, more comprehensive frameworks, such as NIST SP 800-53 or ISO 27002 are required. NIST CSF has the least coverage of the major cybersecurity frameworks. It works great for smaller or unregulated businesses. The NIST CSF is often used as a reporting tool to report security to executive leadership, since the five high-level categories of Identify, Detect, Protect, Respond & Recover make it easier to report complex topics under this perspective.

## Example Cybersecurity Documentation

Below is an example of how a cybersecurity policy links to control objectives, standards and procedures:

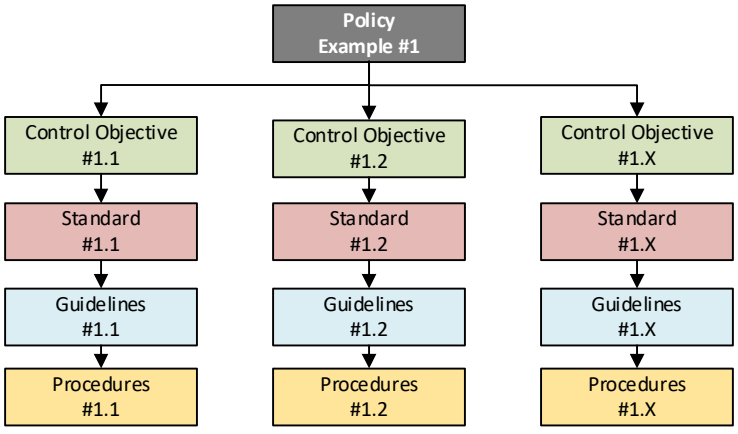
| Documentation Component | Simple Example | |
|---|---|---|
| Policy | *"We will property maintain our network and assets."* | Policies are "high level" statements of management's intent and are intended to guide decisions to achieve rational outcomes. Policies are not meant to be prescriptive, but provide an overall direction for the organization. |
| Control Objective | *"The organization applies software patches in a timely manner."* | Control Objectives support policy by identifying applicable requirements that the organization needs to address. These applicable requirements can be best practices, laws or other legal obligations:<br>- *MA 201 CMR 17.00 – Computer System Security Requirements*<br>- *OR 646A.622 – Technical Security Safeguards*<br>- *PCI DSS – Requirement 6.1* |
| Standard | *"Systems must be patched within 30 days of the vendor's release date."* | Standards establish formal requirements in regards to processes, actions and configurations. Standards are entirely focused on providing narrowly-focused, prescriptive requirements that are quantifiable. |
| Procedure | *"Workstations and servers will be patched on [certain day each month] by [assigned team].* | Procedures are formal methods of performing a task, based on a series of actions conducted in a defined and repeatable manner. |

### Why Cybersecurity Documentation Should Be Scalable

It is imperative that cybersecurity & data privacy documentation be scalable and flexible, so it can adjust to changes in technology, evolving risk and changes within an organization.

The modern approach to cybersecurity & data privacy documentation is being modular, where it is best to link to or reference other documentation, rather than replicated content throughout multiple policy or standard documents. Not only is "traditional model of cybersecurity documentation" inefficient, but it can also be confusing and lead to errors. Additionally, when it comes to audits/assessments, it is true that "time is money" where inefficient, cumbersome documentation has a very real financial cost associated with the amount of time it takes an auditor/assessor to parse through the documentation. Concise, efficient documentation can pay for itself in the cost-savings from a single audit/assessment.

A good example of documentation that is scalable, modular and hierarchical is in the diagram below:



### Educating Users On The Ramifications of Non-Compliance With A Policy or Standard

Part of a complete cybersecurity program includes notifying users about their responsibilities for upholding cybersecurity policies and standards. Additionally, users need to be aware that if a user is found to have violated any policy, standard or procedure that he/she may be subject to disciplinary action, up to and including termination of employment. Depending on what laws and regulations apply to the company, it should also be published that violators of data security or privacy laws may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

### Performing Reviews & Tracking Changes

At least annually, your company's management should review the cybersecurity documentation. This is a common requirement and it is a good opportunity to make improvements, since documentation needs to change over time.

A pretty straightforward approach to managing cybersecurity documentation is the typical "Plan-Do-Check-Act" (**PDCA**), approach where a company operates an ongoing process of evaluation and improvement:

- Plan: This phase involves designing cybersecurity documentation, assessing technology and data-related risks, and selecting appropriate controls.
- Do: This phase involves implementing and publishing cybersecurity documentation.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the cybersecurity program, including violations or exceptions that may have occurred since the last review.
- Act: This has involves making changes, where necessary, to bring the cybersecurity documentation back to optimal performance.

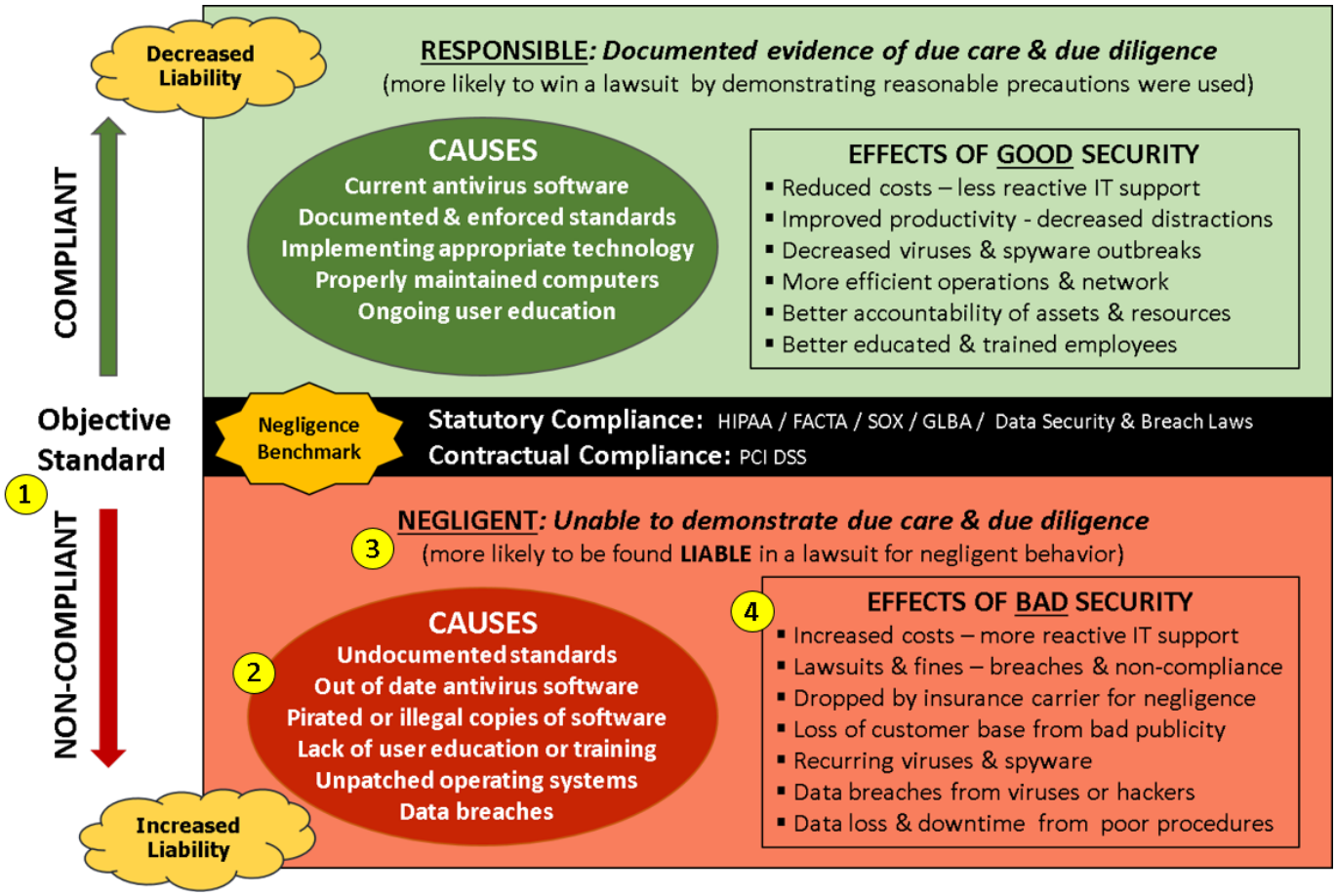
For some companies, it can be a "deep dive" over several days or weeks, where the entire body of cybersecurity policies and standards are reviewed and signed-off by corporate management. Other companies break up the review cycle over the period of a year, such as ¼ being reviewed each quarter so all will be reviewed within a calendar year. It is entirely up to management what works best for each company.

The key thing that needs to be done is to document when the review(s) took place and what changed. There are a lot of ways change logs can be maintained, but it is also important that a process exists to inform employees, contractors and partners of any change that impacts them.

## WHY YOUR COMPANY NEED CYBERSECURITY DOCUMENTATION

### GOOD SECURITY & DATA PRIVACY PRACTICES REDUCE RISK & IMPROVE EFFICIENCIES

The goal of an organization's cybersecurity & data privacy documentation is to build a security-minded culture that decreases liabilities, while at the same time improves operational efficiencies – this equates to bottom-line savings for your company!




1 If your company accepts credit cards, advises on financial matters, provides healthcare services, or maintains any sensitive regulated data (e.g., FCI or CUI) or Personally Identifiable Information (sPII) on clients or employees, then you are responsible for certain compliance requirements. These standards, dictated by the regulation or requirement, establish the objective benchmark for what "reasonably expected" cybersecurity & data privacy controls should be in place.

2 If your company does not meet the minimum standards of a compliance requirement, that deficiency is evidence of negligence. Negligence can be as simple as outdated antivirus software, weak passwords, unencrypted wireless, unpatched operating systems, or inadequate documentation. Ignorance is not an excuse! Negligence can also mean a False Claims Act and/or FTC Act violation.

3 Negligence is demonstrated by a lack of documented due care and due diligence. If you are taken to court, a prosecuting attorney's aim likely will be to prove negligence. Without documented due care and due diligence, the task is made easier to prove negligence and allow damages to be awarded to the plaintiff.

4 The ramifications of being "negligent" can be devastating for a company, since most insurance policies have a "negligence loophole" built in that precludes insurers from having to pay out. The bottom line is your company may have to pay all fines, damages, and legal fees on its own, without any insurance reimbursement. A single negligent event can cause a business to go out of business forever, since liability insurance may not cover professional negligence for cybersecurity-related incidents. The simple rule of thumb is if you are not in compliance with what you are legally obligated to do, then you are professionally negligent.

## Common Cybersecurity Compliance Requirements

The following examples are common compliance concerns that apply to businesses. Some common requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) applies to any business that accepts payment via debit or credit card, regardless of industry or geography.

### HIPAA & PCI DSS Compliance

**Example #1: Physical Therapist**

Compliance Requirements: HIPAA, PCI DSS & State Breach Laws

**Why?** This physical therapist office deals with electronic Protected Health Information (ePHI) of clients so it falls under HIPAA. The office also accepts co-payments by credit card so it falls under PCI DSS. Since the state requires a breach notification plan, the office must also adhere to state-specific compliance requirements for data breaches.

### PCI DSS & GLBA Compliance

**Example #2: Certified Public Accountant (CPA)**

Compliance Requirements: GLBA, PCI DSS & State Breach Laws

**Why?** Like most CPAs, this CPA deals with private financial information of clients, so it falls under GLBA. The CPA works for clients that accept credit cards and has access to their QuickBooks accounts (containing cardholder information), so the CPA must meet PCI DSS requirements. Most states waive state-sponsored breach laws if the company is GLBA compliant, so there may be no additional requirements by the state.

### GLBA & PCI DSS Compliance

**Example #3: Lawyer**

Compliance Requirements: HIPAA, FACTA, GLBA, PCI DSS & State Breach Laws

**Why?** This law offices deal with Protected Health Information (PHI) of clients (injury claims) so it falls under HIPAA. Since the office also performs real estate closings and is responsible for private financial information, it falls under both FACTA and GLBA. The office accepts payment by credit card so it falls under PCI DSS. This state waives its breach notification law if the law office is GLBA compliant, so there may be no additional requirements by the state.

### PCI DSS Compliance for Retailers

**Example #4: Coffee Shop**

Compliance Requirements: PCI DSS

**Why?** This coffee shop accepts payment by credit and debit cards so it falls under PCI DSS. This specific state does not have any specific laws for breach notification, so the coffee shop only has to focus on PCI DSS compliance.

### State Identity Theft Law Compliance

**Example #5: Construction Company**

Compliance Requirements: State Breach Laws

**Why?** The construction company operates in a state that has a law requiring both client and employee sensitive Personal Identifying Information (sPII) to be protected and for notification in the event of a breach.

## What Documentation Solutions Are Available To Your Company

### Hiring A Consultant

Hiring a cybersecurity consultant will provide you with the most customized documentation available. However, at a billable rate of anywhere between $150-300/hr, it can easily cost $30,000-90,000 to outsource the development of a relatively straightforward cybersecurity & data privacy program's documentation.

Generally, the cybersecurity consultant you hire will help navigate you through the selection of leading practices that are right for your business and identify the applicable statutory/regulatory/legal compliance requirements. This is where it can be great to have a professional to assist with this effort, if your company can afford the financial cost and the timeline required to develop it.

### Writing Your Own Documentation

Within a few minutes of performing a search on the Internet for cybersecurity documentation templates, you will likely have a few options for a "do it yourself" approach to writing a cybersecurity policy or entire program for your company. This can range anywhere from reading a book on the topic to purchasing and editing templates you download from the Internet.

Similar to doing your own taxes that can be done without consulting with a CPA, you can write your own cybersecurity documentation. It just comes down to the amount of time you are willing to put into doing documentation yourself and accepting the risk of not having the professional expertise to ensure your solution is comprehensive enough to address your company's needs.

### Hybrid Approach – Semi-Customized Cybersecurity Documentation

Another option available to you is to purchase a "semi-customized" solution. This entails a semi-customized template that contains cybersecurity policies, standards and guidelines based on ISO or NIST best practices, where you just have to customize the documentation for your specific needs.

This is arguably the most efficient solution, when taking into account the expenses of writing your own solution or outsourcing. The "heavy lifting" is done by a cybersecurity professional and you merely perform the final touches for your company's needs.

ComplianceForge's solutions exist in the "semi-customized" solution realm. We did the hard work in researching, writing and editing the content, where you tailor the remaining changes to your specific business needs and technology considerations.