PRACTICAL GUIDE:
UNDERSTANDING INFORMATION SECURITY POLICIES & STANDARDS

Version 2017.1

TABLE OF CONTENTS

ADDRESSES THE THREE-PILLARS OF IT SECURITY – THE "CIA TRIAD"

Protecting the systems that collect, process, and maintain your company's data is of critical importance. Therefore, safeguards must exist to offset possible threats to the confidentiality, integrity and availability of your data and systems. This is considered the "CIA Triad" and it forms the foundation of what IT security measures are implemented to protect:

- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.

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. Since effective security 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 information security requirements to be made available to all users in a format that they can understand. That means your company has to publish those requirements in some manner. Those requirements are most commonly expressed in the form of policies and standards in either PDF format or published to an internal webpage.

WHAT IT SECURITY POLICIES & STANDARDS ARE

In a business context, IT security policies provide direction to all employees and contractors within a company to address needs for IT security requirements. This high-level guidance for IT security needs is intended to be in accordance with the company's business objectives, as well as relevant laws and other legal obligations for data security and privacy.

Unfortunately, for many IT professionals, when they refer to a "policy" they are really meaning a "standard" and that creates a great deal of confusion when people start talking IT security documentation, since those are not interchangeable terms. As you can see from the definitions below, standards are subordinate to policies and standards address the intended requirements needed to satisfy a policy:

- **IT SECURITY POLICY**. A policy is a statement of expectation that clearly identifies management's intent for a specific area of IT security. Policies are intended to guide decisions and achieve rational outcomes that is enforced by standards and further implemented by procedures.
- **IT SECURITY STANDARD**. Standards are formally established requirements in regard to processes, actions, and configurations.

WHAT IT SECURITY POLICIES & STANDARDS ARE NOT

IT security policies & standards are NOT all-encompassing statements of requirements and instruction. This is a common misperception by users and IT professionals, which is due to a fundamental lack of understanding on their part about how IT security documentation is meant to be written in order to develop a comprehensive IT security program, which is really the intent of having documentation in the first place.

This comprehensive coverage only comes from having documentation that is both hierarchical and based on industry-recognized best practices. This is covered in greater detail in this guide, so please continue to read on!

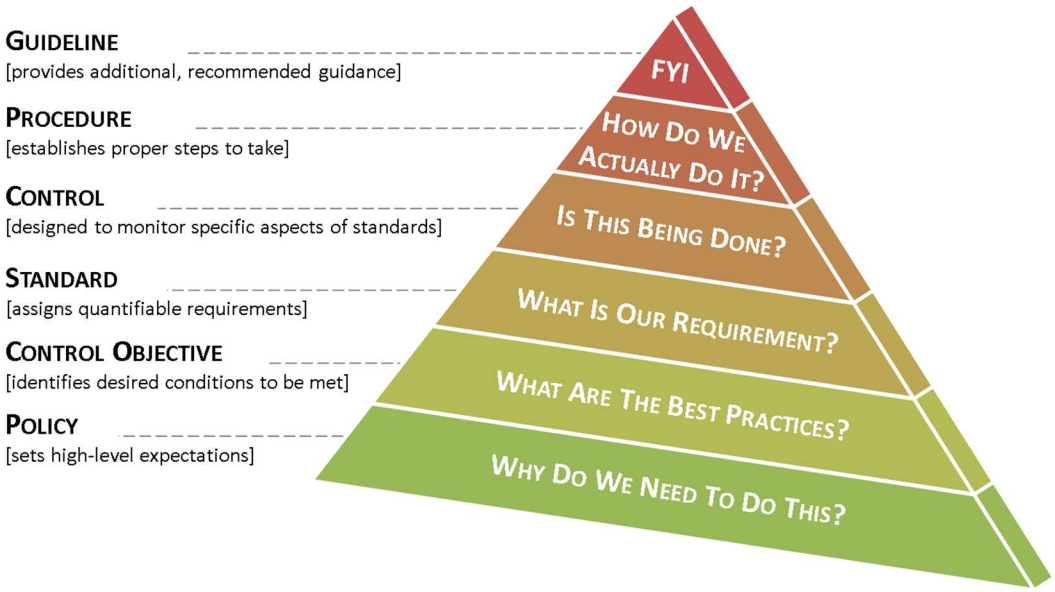
What IT Security Documentation Looks Like When It Is Done Right

The formation of the policies is driven by many factors, with the key factor being risk. These policies set the ground rules under which a company operates and safeguards its data and systems to both reduce risk and minimize the effect of potential incidents. These policies, including their related standards, procedures, and guidelines, are necessary to support the management of information risks in daily operations.

The development of policies provides due care to ensure users understand their day-to-day security responsibilities and the threats that could impact a company. Implementing consistent security documentation will help your company comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity and availability of data and systems.

IT Security 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 of the policy and all of the components of IT security documentation build off each other to make a cohesive approach to addressing a requirement:



Proper information security documentation is comprised of five main parts:

(1) Policy that establishes management's intent
(2) Control Objective that identifies the condition that should be met
(3) Standards that provides quantifiable requirements to be met
(4) Procedures that establish how tasks must be performed to meet the requirements established in standards
(5) Guidelines are recommended, but not mandatory

Understanding The Purpose of IT Security Documentation

The purpose of a company's IT security documentation is to prescribe a comprehensive framework for:

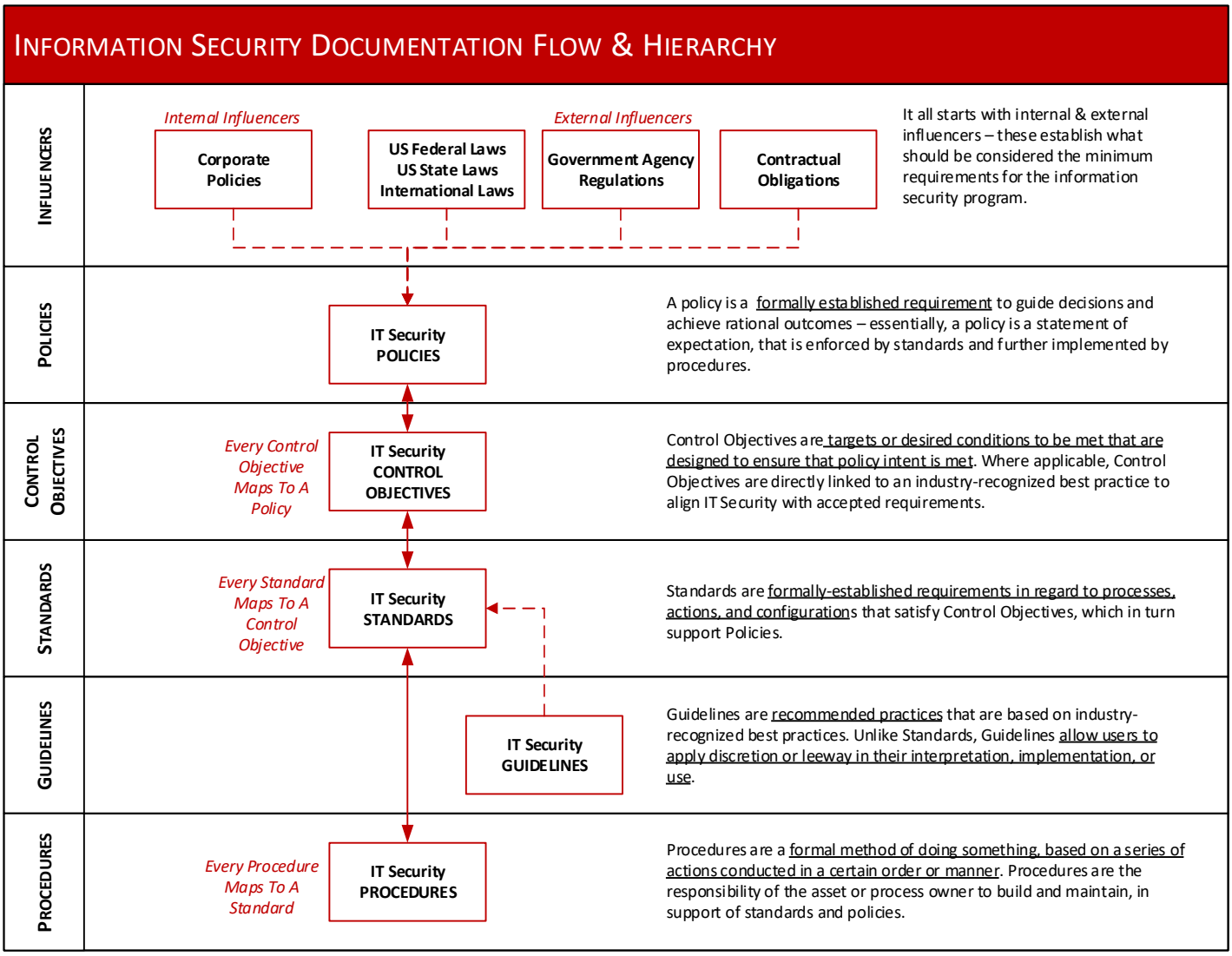
- Creating a clearly articulated approach to how your company handles IT security – in terms of ISO 27001, this concept would be considered an Information Security Management System (ISMS).
- Protecting the confidentiality, integrity, and availability of data and systems on your network.
- Providing guidance to help ensure the effectiveness of security 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 IT security risks.

IT Security Documentation Hierarchy – Understanding How IT Security Documentation Is Connected

It all starts with influencers – these influencers set the tone and establish what is considered to be due care for information security 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

When that is all laid out properly, your company's IT security documentation show flow like this:



Defining The Scope & Applicability of IT Security Policies & Standards

Defining the scope for an IT security program is pretty easy - a company's IT security policies, standards and procedures should apply to all of its data, systems, activities, and assets owned, leased, controlled, or used by the company. This also includes its contractors and/ or other business partners on behalf of the company.

Additionally, the scope of a company's IT security documentation should apply to all employees, contractors, sub-contractors, and their respective facilities supporting the company's business operations, wherever the company's data is stored or processed, including any third-party contracted by the company to handle, process, transmit, store, or dispose of data.

EXAMPLE IT SECURITY DOCUMENTATION

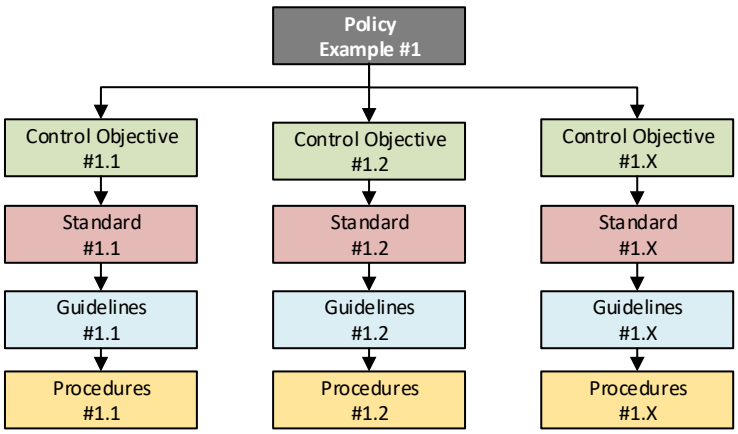
Below is an example of how an IT security policy links to control objectives, standards and procedures:

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: - *MA 201 CMR 17.00 – Computer System Security Requirements* - *OR 646A.622 – Technical Security Safeguards* - *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 IT SECURITY DOCUMENTATION SHOULD BE SCALABLE

It is imperative that IT security documentation be scalable and flexible, so it can adjust to changes in technology, evolving risk and changes within your organization. Part of this approach is being modular, where it is best to link to or reference requirements, rather than have similar content replicated throughout multiple IT security policy or standard documents. Not only is this inefficient, it can be confusing and lead to errors. A good example of that is by not having a single source for password length, multiple conflicting requirements can exist within IT security documentation (e.g., the requirement is only documented in the Authentication Standard under the Access Control Policy).

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



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

Part of a complete IT security program includes notifying users about their responsibilities for upholding IT security 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 IT security documentation. This is a pretty common requirement (e.g., PCI DSS) and it is a good opportunity to make improvements, since documentation needs do change over time.

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

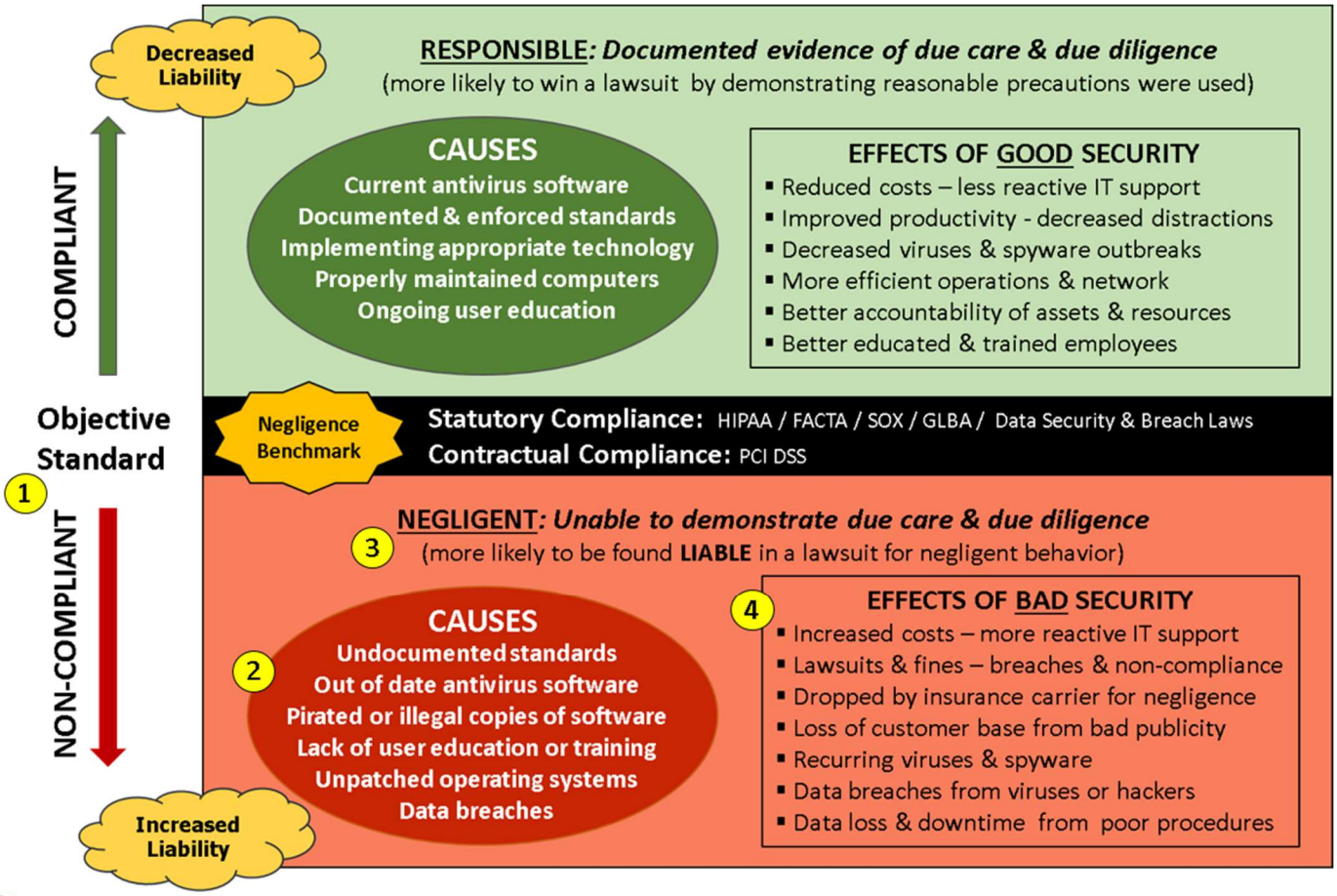
- Plan: This phase involves designing the IT security documentation, assessing IT-related risks, and selecting appropriate controls.
- Do: This phase involves implementing and publishing the IT security documentation.
- Check: This phase involves reviewing and evaluating the performance (efficiency and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

For some companies, it can be a "deep dive" over several days where the entire body of IT security policies and standards are reviewed and signed-off by 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 for what works best for their company.

The key thing that needs to be done is document when the review(s) took place and what actually 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.

GOOD IT SECURITY REDUCES RISK & IMPROVES EFFICIENCIES

The goal of IT security documentation is to build an IT security program for your company 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 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" IT security protections 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 IT security documentation. Ignorance is not an excuse!

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 IT security-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 IT Security 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 its 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.

DEFINING THE ACCEPTED FRAMEWORKS FOR IT SECURITY

When it really comes down to it, there are very few frameworks for IT security that are commonly accepted as "best practices" and those are listed below:

- NIST 800-53
- ISO 27001/27002
- COBIT 5

If you ask an IT security professional to identify their preferred best practice, 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 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 IT security's two heavy hitters – NIST and ISO. These frameworks both cover the same fundamental building blocks of an IT security program, but differ in some content and layout. Both can be perfect solutions, but each one has its benefits and drawbacks, so choice should be driven by the type of industry your business is in.

Keep in mind that all of the best practice frameworks were written by committee and none of them are perfect!

NIST 800-53

The National Institute of Standards and Technology (NIST) is on the fourth revision (rev4) of Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Notice that doesn't mention anything about private industry – NIST designed this framework to protect the US federal government. However, due to the significant outsourcing to private companies, as well as extensive regulation for businesses, NIST 800-53 best practices have become the de facto standard for private businesses that do business with the US federal government.

The Federal Information Security Management Act (FISMA) and the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) rely on the NIST 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 800-171, P*rotecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST 800-53 is called out as the best practices for government contractors to secure their systems. That further helps strengthen NIST 800-53 as a best practice within the US, especially for any government contractors.

One great thing about NIST 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 27001/27002

The International Organization for Standards (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 aides in the implementation of ISO 27001.

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 800-53, which has an advantage of being less complex and therefore easier implement.

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.

COBIT

The Control Objectives for Information and Related Technology (COBIT) 5 for Information Security is a framework created by the Information Systems Audit and Control Association (ISACA) and it is intended for IT governance.

In theory, COBIT can be beneficial in the high-level development of an IT security program, especially for a larger, publicly-traded company. In reality, while COBIT has good ideas, it fails to offer the details available by NIST or ISO. For this reason, COBIT realistically earns an honorable mention, as compared to practical frameworks such as NIST and ISO. It is very unlikely you will encounter a company that uses the COBIT framework for its information security program, other than referencing it in an effort to demonstrate alignment with COBIT for compliance requirements, such as the Sarbanes Oxley Act (SOX).

Similar to ISO, ISACA charges for its publications - http://www.isaca.org/cobit/pages/info-sec.aspx

SUPPORTING FRAMEWORKS

As technology continues to evolve, there are numerous specializations that have popped up and several have formed their own specific best practices. These specializations are sometimes are needed to be referenced to support the major IT security best practices. For a few examples of specializations that these best practices would leverage:

- A standard that calls out "cloud security" might need to leverage the Cloud Security Alliance (CSA) for specific requirements.
- A standard that calls out secure software development might need to leverage the Open Web Application Security Project (OWASP) for specific requirements.

CLOUD SECURITY ALLIANCE (CSA) – CLOUD CONTROLS MATRIX (CCM)

The CSA CCM is specifically designed to reinforce IT security best practices to secure "the cloud" for both vendors and customers. The foundations of the CSA CCM rest on its relationship to industry-accepted IT security standards, such as NIST, ISO & COBIT. The CSA CCM strengthens existing IT security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

OWASP is a not-for-profit organization focused on improving the level of security for software. OWASP does not endorse or recommend commercial products or services, allowing it to remain vendor-neutral. The focus is to identify the most current best practices around secure software development.

What Documentation Solutions Are Available To Your Company

Hiring A Consultant

Hiring an IT security 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 $10,000-20,000 to outsource the development of a relatively straightforward IT security program's documentation.

Generally, the IT security consultant you hire will help navigate you through the selection of best 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, if you can afford it.

Writing Your Own Documentation

Within a few minutes of performing a search on the Internet for IT security documentation templates, you will likely have a few options for a "do it yourself" approach to writing an IT security 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 IT security 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 IT Security Documentation

Another option available to you is to purchase a "semi-customized" solution. This entails a semi-customized template that contains IT security 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 an IT security professional and you merely perform the final touches for your company's needs.