NIST 800-171

COMPLIANCE SCOPING GUIDE

COMPLIANCE FORGE

Version 2017.2

Disclaimer: This document is provided for REFERENCE purposes only. It does not render professional services and is not a substitute for professional services. If you have compliance questions, you should consult an information security professional.

TABLE OF CONTENTS

Executive Summary

This document is intended to help companies comply with NIST 800-171. Part of the process of becoming compliant with this regulation is understanding the scope of the **Controlled Unclassified Information (CUI)** environment.

Given that there are similarities between scoping for NIST 800-171 and the Payment Card Industry Data Security Standard (PCI DSS), we leveraged the outstanding concepts that the Open Scoping Framework Group applied to PCI DSS compliance with the *Open PCI DSS Scoping Toolkit*[1] and applied that similar methodology to NIST 800-171.

When you look at NIST 800-171 compliance scoping, it has some similarities to PCI DSS:

- PCI DSS is focused on protecting the Cardholder Data Environment (CDE), which is where payment card data is stored, processed and transmitted.
- NIST 800-171 is focused on protecting the CUI environment, which is where sensitive data (in regards to US national security) is stored, processed or transmitted.

From the perspective of PCI DSS, if scoping is done poorly, a company's entire network may be in-scope as the CDE, which means PCI DSS requirements would apply uniformly throughout the entire company. In these scenarios, PCI DSS compliance can be prohibitively expensive or even technically impossible. However, when the network is intelligently-designed with security in mind, the CDE can be a small fraction of the company's network, which makes compliance much more achievable and affordable. We feel that NIST 800-171 should be viewed in the very same manner.

This guide is not endorsed by the National Institute of Science and Technology (NIST) or any other organization. This is merely an unofficial guide that ComplianceForge.com compiled to help companies comply with NIST 800-171.

If you are unsure what CUI is, we highly recommend that you visit the US government's authority on the matter, the **US Archive's CUI Registry** - https://www.archives.gov/cui/registry.

[1] Open PCI DSS Scoping Toolkit - https://www.isaca.org/Groups/Professional-English/pci-compliance/GroupDocuments/OpenPCIScopingToolkit.pdf

UNDERSTANDING THE INTENT OF NIST 800-171

If you are new to NIST 800-171, it is intended to help "non-federal entities" (e.g., government contractors) to comply with reasonably-expected security requirements by using the systems and practices that government contractors already have in place, rather than trying to use government-specific approaches.

NIST 800-171 also provides a standardized and uniform set of requirements for all **Controlled Unclassified Information (CUI)** security needs, tailored to non-federal systems, allowing government contractors to comply and consistently implement safeguards for the protection of CUI. When it comes down to it, NIST 800-171 is designed to address common deficiencies in managing and protecting unclassified information.

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

NIST 800-171 requires private companies to protect the confidentiality of CUI.

The CUI requirements within NIST 800-171 are directly linked to **NIST 800-53 MODERATE baseline controls** and are intended for use by federal agencies in contracts or other agreements established between those agencies and government/DoD contractors, as it applies to:

- When CUI is resident in non-federal information systems and organizations;
- When information systems where CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and
- Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry.

SUCCESSFUL NIST 800-171 COMPLIANCE ADDRESSES THE "CIA TRIAD"

Protecting the systems that process, store and transmit CUI is of critical importance. Therefore, safeguards must exist to offset possible threats to the confidentiality, integrity and availability of CUI and the systems that enable access to it. This is considered the "CIA Triad" and it forms the foundation of what IT security measures are implemented to protect:

CONFIDENTIALITY
INTEGRITY
C-I-A
TRIAD
AVAILABILITY

- **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.

SCOPING NIST 800-171

This guide provides a structured method for determining which system components in a company's environment are within scope for NIST 800-171 compliance. This guide categorizes system components according to several factors:

- Whether CUI is being stored, processed or transmitted;
- The functionality that the system component provides (e.g. access control, logging, antimalware, etc.); and
- The connectivity between the system component and the CUI environment.

Please note that the use of this guide necessitates that your company has already located and documented where CUI is stored, processed and transmitted. This also assumes that documentation exists for relevant business process work flows and data flows, since that is needed to fully understand the physical and logical computing environments, as well as existing controls that are in place to protect CUI.

This guide can be used by both large and small companies to help critically evaluate the system components that comprise the scope of assessment. The primary difference between large and small companies will be the number of system components that are evaluated.

WHAT THIS GUIDE ADDRESSES

This guide helps with the following:

- Aids in determining which system components fall in and out of scope;
- Facilitates communication between companies and assessors by providing a common language to describe the computing environment and risks to CUI;
- Provides a framework to categorize and identify the different types of system components, each with a different risk profile associated with it; and
- Provides a thought process to reduce the scope of assessment by:
  - Isolating and controlling access to CUI;
  - Re-architecting the control environment; or
  - Implementing further controls.

WHAT THIS GUIDE DOES NOT ADDRESS

Although addressing the people and processes around CUI is a necessary part of any NIST 800-171 compliance program, this guide focuses on categorizing the system components that comprise a company's computing environment.

In addition, this guide does not define what NIST 800-171 controls are required for each category. Because every company is different, it is up to each company and its assessor to determine the nature, extent and effectiveness of each control to adequately mitigate the risks to CUI.

SEGMENTATION CONSIDERATIONS

Network segmentation should be viewed as a process to isolate system components that store, process, or transmit CUI from systems that do not. Adequate network segmentation may reduce the scope of the CUI environment and overall reduce the scope of a NIST 800-171 audit.

To eliminate ambiguity surrounging the term "segmentation" in terms of NIST 800-171 scoping, this guide uses one of the two following terms:

- Isolation – This is achieved when network traffic between two system components is not permitted.
- Controlled Access – This is achieved when access between system components is restricted to defined parameters.
  - Controlled access is more common than isolation.
  - Restrictions may include logical access control, traffic type (e.g., port, protocol or service), the direction from which the connection is initiated (e.g., inbound, outbound), etc.

Mechanisms providing the isolation or controlled access functionality may be either logical or physical. Examples of mechanisms include network and host-based firewalls, virtual routing and switching appliances, and access control lists.

NIST 800-171 Compliance Lifecycle

The table below outlines the key milestones in achieving and maintaining compliance with NIST 800-171 requirements, as well as how this guide fits into that lifecycle.

Steps BEFORE You Use The Guide	
Confirm the Accuracy of the Assessment Scope	#1. Document the company's business processes and data workflows for known and potential instances where CUI is stored, processed, or transmitted. After gaining a complete understanding of all people, process, and technology-related interactions with CUI, identify and document all locations and flows of CUI across the organization.
Evaluate the Business Need for Each Location and Flow of CUI	#2. For each instance identified above, evaluate the business need to handle CUI: ▪ If CUI is not needed, stop collecting it and securely delete what has been collected. ▪ If CUI is required, consider migrating or consolidating it elsewhere in the CUI environment to reduce scope, improve control, and mitigate risk.
Steps To Use The Guide	
Use the Decision Tree to Categorize Systems	#3. Use the **Scoping Decision Tree** to determine whether each system component is in the scope of assessment, and assign it a specific scoping sub- category. *Note: The result of categorizing each system component helps identify the relevant risks to the CUI environment. Completing this step can be used in support of NIST 800-171 requirement 3.11 (e.g., periodically assess the risk to organizational operations)*
Steps To Follow AFTER Using The Guide	
Evaluate Scoping Conclusions and Consider Further Reducing the Scope of Assessment	#4. Consider the risk implications of the scoping conclusions and identify potential opportunities to further reduce assessment scope (e.g., re-architecting business processes, data flows, and/or the control environment).
	#5. Evaluate each in-scope system component against all NIST 800-171 requirements for applicability and necessity, based on the risk to CUI and the overall control environment.
	#6. Architect, design, implement and document the controls required to adequately mitigate the identified risk to CUI.
	#7. Assess the controls for design and operating effectiveness, at the level of both the system components and the environment.

Scoping Categories

When it comes down to it, the CUI environment encompasses the people, processes and technology that stores, processes or transmits CUI.

- Store – When CUI is inactive or at rest (e.g., located on electronic media, system component memory, paper)
- Process – When CUI is actively being used by a system component (e.g., entered, edited, manipulated, printed, viewed)
- Transmit – When CUI is being transferred from one location to another (e.g., data in motion).

Scoping Categories

NIST categorizes system components as being either in or out of the scope for NIST 800-171, so there is no official guidance at a more granular-level. Given that lack of guidance and a need for businesses to demonstrate both due care and due diligence with their NIST 800-171 compliance operations, this guide defines three (3) categories of system components and highlights the different types of risks associated with each category. This approach makes it more evident which system components are the most important to protect, based on the types of risk posed to CUI.

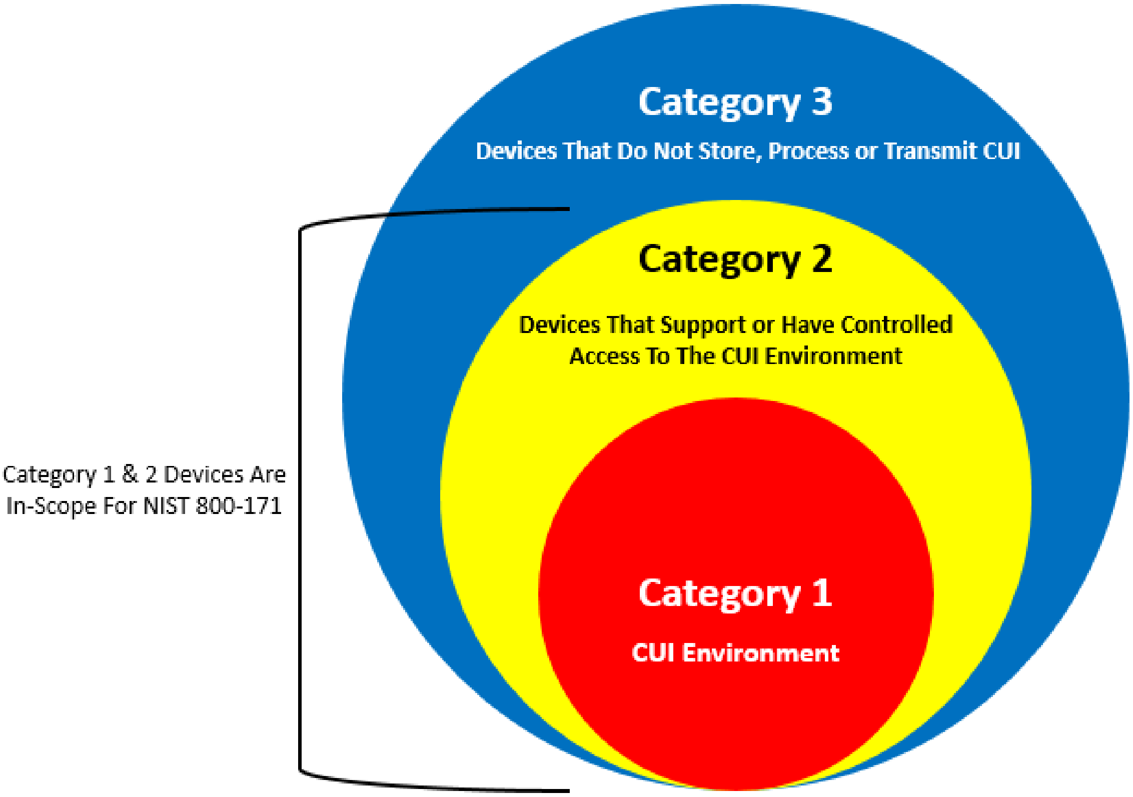
Every system component within a company's computing environment can be categorized into one and only one of the following:

- Category 1 – System components that process, store or transmit CUI or are not isolated or restricted through controlled access from other Category 1 system components.
- Category 2 – System components that have controlled access to a Category 1 system component.
- Category 3 – System components that are isolated from all Category 1 system components.

Categorizing each system component into one of these categories achieves several key results:

- Identifies all system components that are within the scope of NIST 800-171 compliance;
- Aids in documenting risks to CUI as each system component within the environment is analyzed;
- As Category 2 system components are further sub-categorized, helps clarify risks to CUI; and
- Enables the objective evaluation of CUI controls for applicability and necessity.

The following graphic shows the three, mutually exclusive categories:


Category 3
Devices That Do Not Store, Process or Transmit CUI
Category 2
Devices That Support or Have Controlled Access To The CUI Environment
Category 1
CUI Environment
Category 1 & 2 Devices Are In-Scope For NIST 800-171

CATEGORY 1 SYSTEM COMPONENTS

A system component is considered Category 1 if it stores, transmits or processes CUI.

Additionally, this guide introduces the concept of "infectious" to address the impact of a Category 1 system component on other devices.

- A system component that stores, processes or transmits CUI (i.e., Category 1a) is said to be "infectious" since it may pull other systems into scope.
- All system components that have unrestricted network access to that Category 1a device become Category 1b devices, even if they do not store, process or transmit CUI (essentially, they are "infected" with compliance requirements).

With this in mind, system components that fall into Category 1 include:

Category	Description
1a	Devices that store, process or transmit CUI.
1b	Devices that do not store, process or transmit CUI, but, are "infected by" Category 1a devices due to the absence of controlled access or isolation.

Implications of Category 1 system components:

- All Category 1 system components are "infectious" towards other non-isolated systems;
- All Category 1 system components are always within the scope of NIST 800-171;
- Each Category 1 system component must be evaluated against all NIST 800-171 requirements to determine the applicability of each requirement; and
- All applicable NIST 800-171 control requirements are necessary for every Category 1 device.

CATEGORY 2 SYSTEM COMPONENTS

Category 2 system components do not store, process or transmit CUI but have controlled access to and/or from Category 1 devices.

This controlled access must:

- Limit network traffic to only that which is required for business operations; and
- Be justified and documented.

With this in mind, system components that fall into Category 2 include:

Category	Description
2a	System components which, through controlled access, provide security services (e.g., Active Directory, remote access, centralized antimalware, logging, monitoring, IPS/IDS, etc.) to a Category 1 device.
2b	System components which, through controlled access, can initiate an inbound connection to a Category 1 device.
2c	System components which, through controlled access, can only receive a connection from a Category 1 device (i.e., cannot initiate a connection).
2x	System components which, through indirect and controlled access, have the ability to administer Category 1 devices. *Note: Category 2x devices have no direct access to/from Category 1 devices.*

Implications of Category 2 system components:

- Category 2 system components have controlled access to the CUI environment;
- Category 2 system components are not "infectious;"
- Category 2 system components are always within the scope of NIST 800-171;

- Each Category 2 system component must be evaluated against all NIST 800-171 requirements to determine the "applicability" of each requirement, as well as the "necessity" of each control based on an assessment of the risk to the CUI environment and the overall control environment.
- Category 2 system components must be adequately protected to prevent Category 3 devices from being a valid vector of attack.

CATEGORY 3 SYSTEM COMPONENTS

Category 3 system components:

- Do not store, process or transmit CUI;
- Are isolated from; and
- Do not provide any services to any Category 1 device.

Therefore, Category 3 system components are not in the scope of NIST 800-171.

SUMMARY OF CATEGORIES

The following table summarizes the scoping categories and sub-categories:

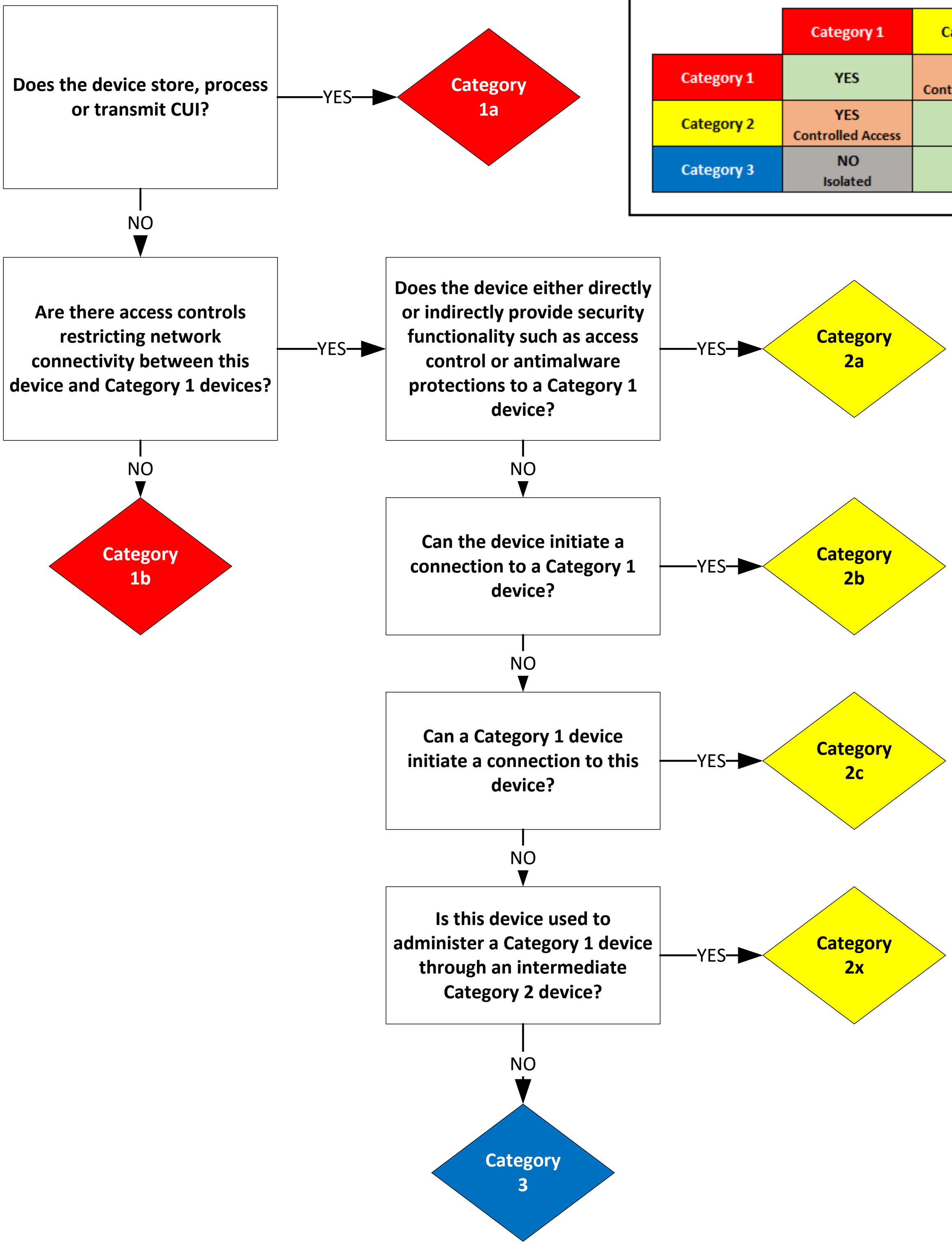
Category	Description	Method of Segmentation	CUI?	Vector of Attack?	In Scope for NIST 800-171?
1a	Devices that store, process or transmit CUI.	N/A	**YES**	**YES**	**YES**
1b	Devices that do not store, process or transmit CUI, but, are "infected by" Category 1a devices due to the absence of controlled access or isolation.	N/A	NO	**YES**	**YES**
2a	System components which, through controlled access, provide security services (e.g., authentication) to a Category 1 device.	Controlled Access	NO	**YES**	**YES**
2b	System components which, through controlled access, can initiate an inbound connection to a Category 1 device.	Controlled Access	NO	**YES**	**YES**
2c	System components which, through controlled access, can only receive a connection from a Category 1 device (i.e., cannot initiate a connection).	Controlled Access	NO	**YES**	**YES**
2x	System components which, through indirect and controlled access, have the ability to administer Category 1 devices.	Controlled Access	NO	**YES**	**YES**
3	Systems that do not store, process or transmit CUI. All network traffic between Category 3 and Category 1 devices is restricted (isolated).	Isolated	NO	NO	NO

Scoping Decision Tree

The following diagram shows the detailed decision tree which applies the concepts introduced in the previous sections.

Communications Allows Between Categories

	Category 1	Category 2	Category 3
Category 1	YES	YES Controlled Access	NO Isolated
Category 2	YES Controlled Access	YES	YES
Category 3	NO Isolated	YES	YES


Does the device store, process or transmit CUI?
YES
Category 1a
NO
Are there access controls restricting network connectivity between this device and Category 1 devices?
YES
NO
Category 1b
Does the device either directly or indirectly provide security functionality such as access control or antimalware protections to a Category 1 device?
YES
Category 2a
NO
Can the device initiate a connection to a Category 1 device?
YES
Category 2b
NO
Can a Category 1 device initiate a connection to this device?
YES
Category 2c
NO
Is this device used to administer a Category 1 device through an intermediate Category 2 device?
YES
Category 2x
NO
Category 3

GLOSSARY: ACRONYMS & DEFINITIONS

ACRONYMS

PDCA. Plan-Do-Check-Act
CDE. Cardholder Data Environment
CERT. Computer Emergency Response Team
CIRT. Computer Incident Response Team
CUI. Controlled Unclassified Information (CUI)
DRP. Disaster Recovery Plan
IRP. Incident Response Plan
ISMS. Information Security Management System
NIST. National Institute of Standards and Technology
PCI DSS. Payment Card Industry Data Security Standard

DEFINITIONS

The National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Information Security Terms*, is the approved reference document used to define common IT security terms. [2]

[2] NIST IR 7298 - http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

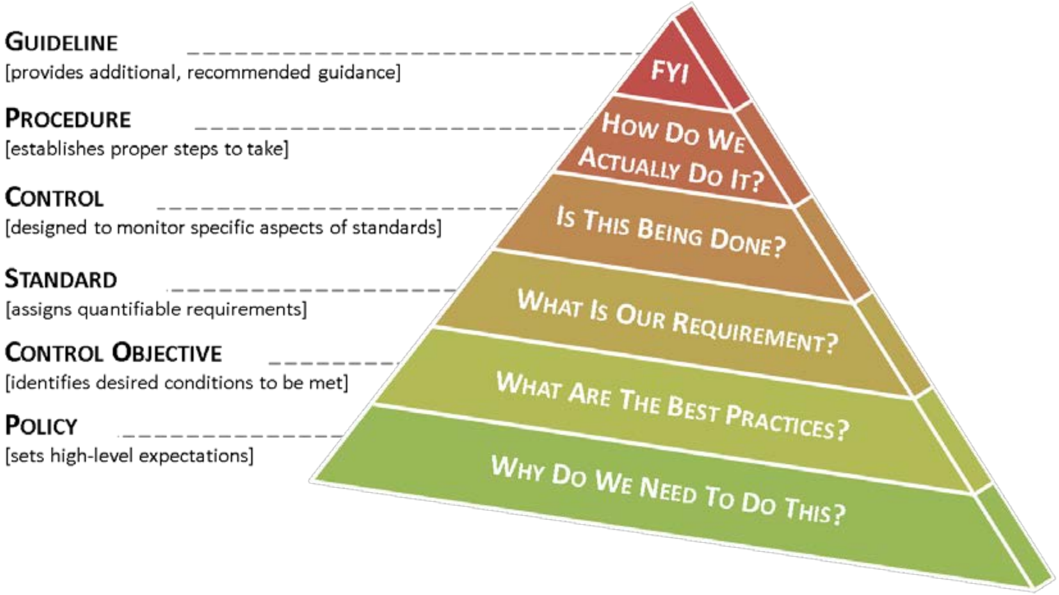
APPENDIX A – DOCUMENTATION TO SUPPORT NIST 800-171 COMPLIANCE

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:


GUIDELINE
[provides additional, recommended guidance]
PROCEDURE
[establishes proper steps to take]
CONTROL
[designed to monitor specific aspects of standards]
STANDARD
[assigns quantifiable requirements]
CONTROL OBJECTIVE
[identifies desired conditions to be met]
POLICY
[sets high-level expectations]
FYI
HOW DO WE ACTUALLY DO IT?
IS THIS BEING DONE?
WHAT IS OUR REQUIREMENT?
WHAT ARE THE BEST PRACTICES?
WHY DO WE NEED TO DO THIS?

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:

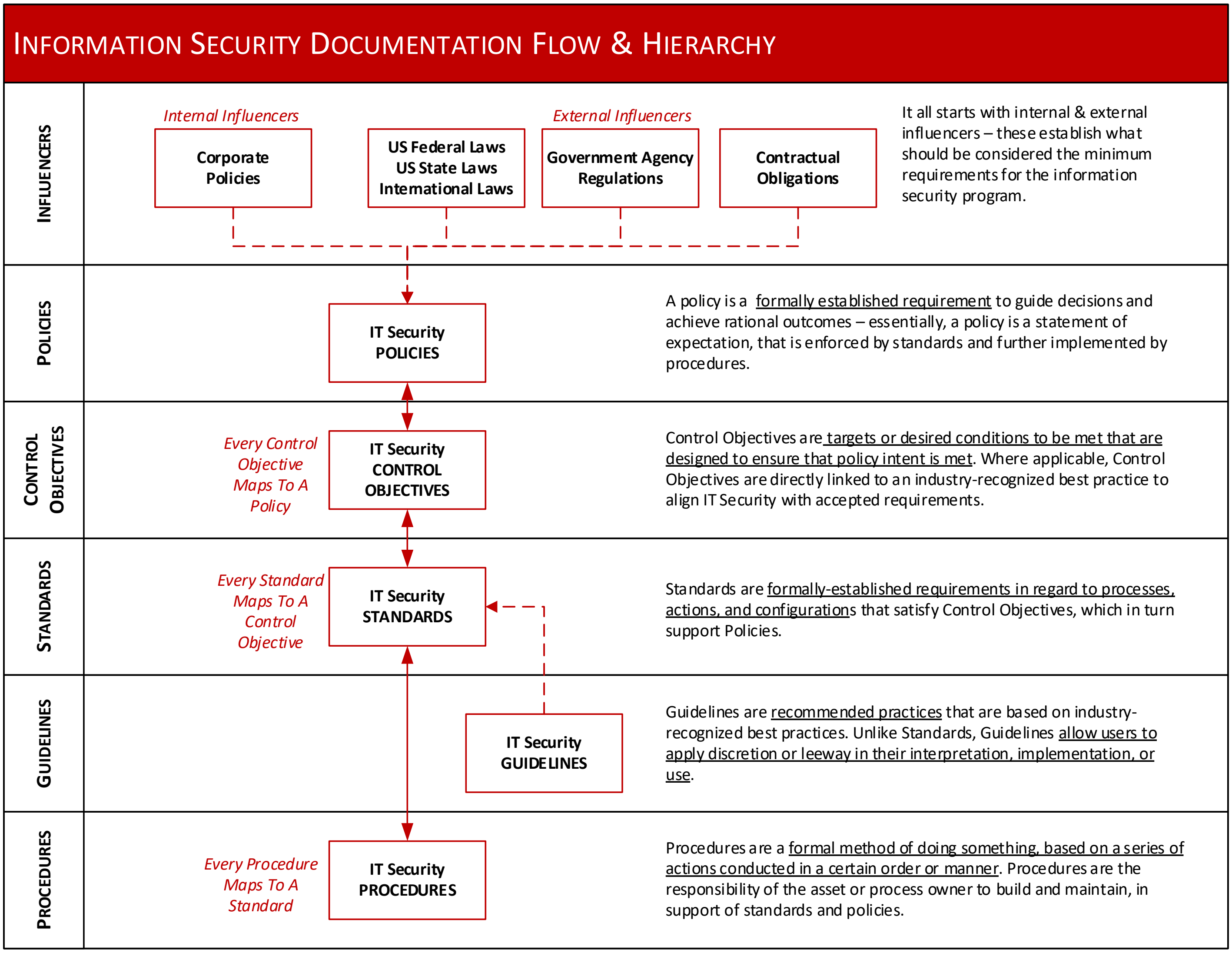
- Creating a clearly articulated approach to how your company handles IT security – in terms of ISO 27001 or NIST 800-53, this concept would be considered an Information Security Management System (ISMS).
- Protecting the confidentiality, integrity, and availability of data and systems on your network.
- 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:



Information Security Documentation Flow & Hierarchy

It all starts with internal & external influencers – these establish what should be considered the minimum requirements for the information security program.

A policy is a formally established requirement 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.

Control Objectives are targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized best practice to align IT Security with accepted requirements.

Standards are formally-established requirements in regard to processes, actions, and configurations that satisfy Control Objectives, which in turn support Policies.

Guidelines are recommended practices that are based on industry-recognized best practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

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 or process owner to build and maintain, in support of standards and policies.

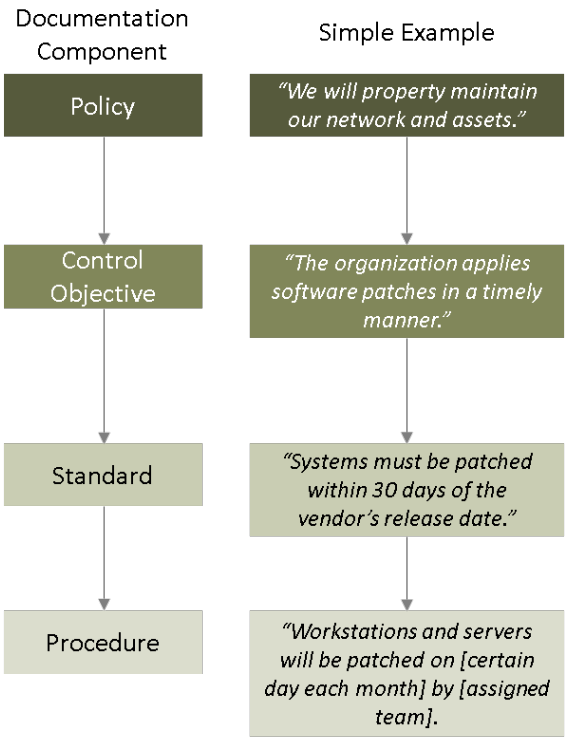
Defining The Scope & Applicability of IT Security Policies & Standards

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:

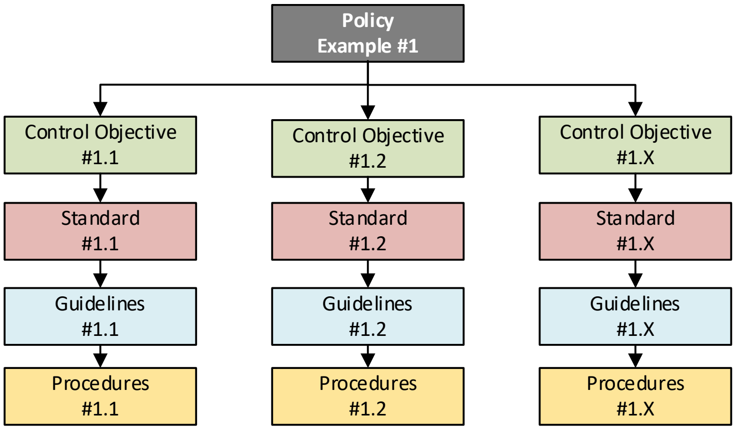


Documentation Component	Simple Example	
Policy	*"We will property maintain our network and assets."*	Policies are "high level" statements of management's intent and are intended to guide decisions to achieve rational outcomes. Policies are not meant to be prescriptive, but provide an overall direction 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 company. 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.