COMPLIANCE FORGE

SCF | SECURE CONTROLS FRAMEWORK

Security & Privacy Risk Management Model (SP-RMM) Overview

SP-RMM

Version 2021.1

Table of Contents

EXECUTIVE SUMMARY

RISK MANAGEMENT BASICS

The concept of creating the Security & Privacy Risk Management Model (**SP-RMM**) was to create an efficient methodology to identify, assess, report and mitigate risk.

The most important concept to understand in cybersecurity and privacy-related risk management is that the cybersecurity and IT departments generally do not "own" technology-related risks, since that "risk ownership" primarily resides with Line of Business (**LOB**) management. An organization's cybersecurity and privacy functions serve as the primary mechanism to educate those LOB stakeholders on identified risks and provide possible risk treatment solutions. Right or wrong, LOB management is ultimately responsible to decide how risk is to be handled.

Where the SP-RMM exists is to help cybersecurity and privacy functions create a repeatable methodology to identify, assess, report and mitigate risk. This is based on the understanding that the responsibility to approve a risk treatment solution rests with the management of the LOB/department/team/stakeholder that "owns" the risk. The SP-RMM is meant to guide the decision to one of these common risk treatment options:

- Reduce the risk to an acceptable level;
- Avoid the risk;
- Transfer the risk to another party; or
- Accept the risk

It is a common problem for individuals who are directly impacted by risk to simply claim, *"I accept the risk"* in a misplaced maneuver to make the risk go away, so that the project/initiative can proceed without having to first address deficiencies. This is why it is critically important that as part of a risk management program to identify the various levels of management who have the legitimate authority to make risk management decisions. This can help prevent low-level managers from recklessly accepting risk that should be reserved for more senior management.

WHY YOU SHOULD CARE

Before you read further, ask yourself these two questions about your organization and your personal exposure in risk management:

1. Can you prove that the right people within your organization are both aware of risks and have taken direct responsibility for mitigating those risks?
2. If there was a breach or incident that is due to identified risks that went unmitigated, where does the "finger pointing" for blame immediately go to?

If you worry about having to preface risk management discussions with, *"Don't shoot the messenger!"* then the SP-RMM can be an additional layer of protection for your professional reputation. Where the SP-RMM benefits security, technology and privacy personnel is the potential "get out of jail" documentation that quality risk assessments and risk management practices can provide. Just like with compliance documentation, if risk management discussions are not documented then risk management practices do not exist.

Instead of executive leadership hanging blame on the CIO or CISO, quality risk management documentation can prove that reasonable steps were taken to identify, assess, report and mitigate risk. This type of documentation can provide evidence of due diligence and due care on the part of the CIO/CISO/CRO, which firmly puts the responsibility back on the management of the team/department/line of business that "owns" the risk.

The SP-RMM is designed to be an integral tool of an organization's ability to demonstrate evidence of due diligence and due care. This not only benefits your organization by having solid risk management practices, but it can also serve as a way to reduce risk for those who have to initiate the hard discussions on risk management topics.

SECURITY & PRIVACY RISK MANAGEMENT MODEL (SP-RMM)

The concept of creating the SP-RMM was to create an efficient methodology to identify, assess, report and mitigate risk. This project was approached from the perspective of asking the question, "*How should I management risk?*" and was a collaboration between ComplianceForge and the Secure Controls Framework (SCF).

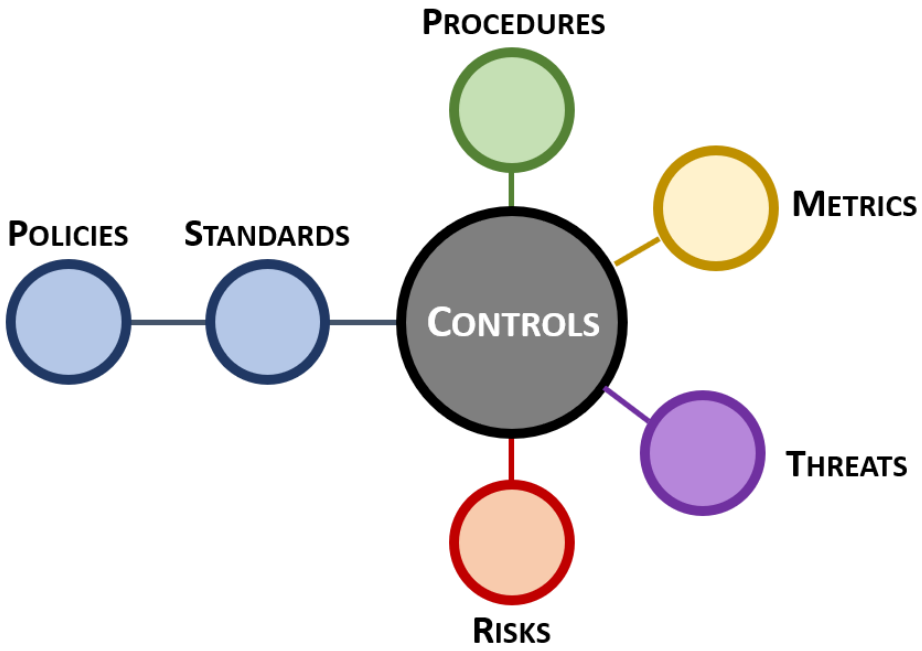
RISKS & THREATS DO NOT EXIST IN A VACUUM

Based on the applicable statutory, regulatory and contractual obligations that impact the scope of a risk assessment, an organization is expected to have an applicable set of cybersecurity and privacy controls to cover those fundamental compliance obligations. That set of controls identifies the in-scope requirements that must be evaluated to determine what risk exists. This is generally considered to be a "gap assessment" where the assessor:

- Evaluates those controls based on the entity's THREAT CATALOG to identify current or potential control deficiencies; and
- Utilize the RISK CATALOG to identify the applicable risks, based on the identified control deficiencies.

Therefore, it is vitally important to understand that risks and threats do not exist in a vacuum. If your cybersecurity and privacy program is appropriately built, you will have a robust controls framework where risks and threats will map directly to controls. Why is this?

- Controls are central to managing risks, threats procedures and metrics.
- Risks, threats, metrics and procedures need to map into the controls, which then map to standards and policies.



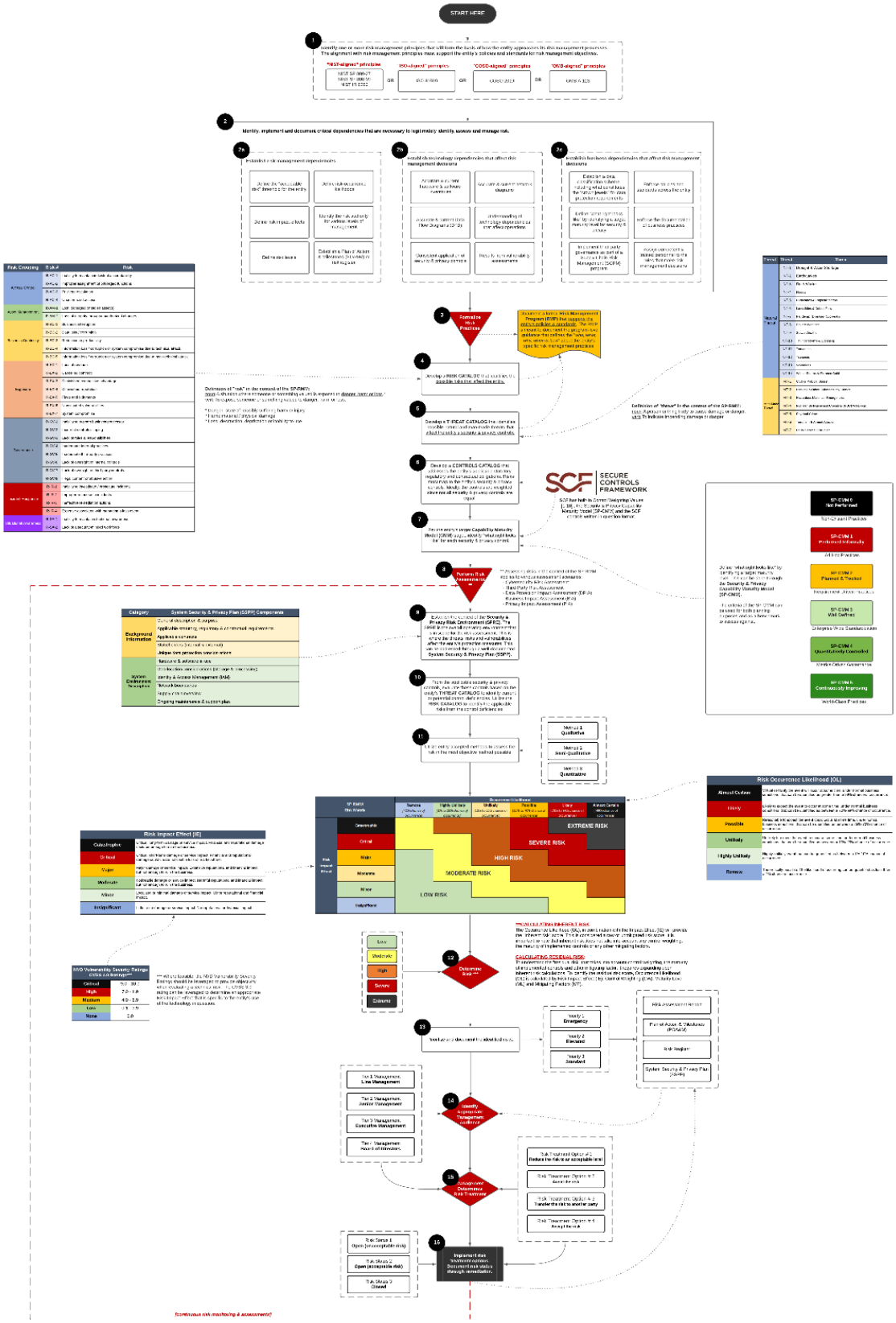
In risk management, the old adage is applicable that "the path to hell is paved with good intentions." Often, risk management personnel are tasked with creating risk assessments and questions to ask without having a centralized set of organization-wide cybersecurity and privacy controls to work from. This generally leads to risk teams making up risks and asking questions that are not supported by the organization's policies and standards. For example, an organization is an "ISO shop" that operates an ISO 27002-based Information Security Management System (**ISMS**) to govern its policies and standards, but its risk team is asking questions about NIST SP 800-53 or NIST SP 800-171 controls that are not applicable to the organization.

This scenario of "making up risks" points to a few security program governance issues:

- If the need for additional controls to cover risks is legitimate, then the organization is improperly scoped and does not have the appropriate cybersecurity and privacy controls to address its applicable statutory, regulatory, contractual or industry-expected practices.
- If the organization is properly scoped, then the risk team is essentially making up requirements that are not supported by the organization's policies and standards.

COVERAGE FROM START TO FINISH

The SP-RMM addresses risk management from how you start building a risk management program through the ongoing risk management practices that are expected within your organization.



[image is downloadable from https://www.securecontrolsframework.com/sp-rmm]

SP-RMM: Steps To Identify, Assess, Report & Mitigate Risk

The SP-RMM is broken down into sixteen (16) steps (note - these steps correspond to the diagram from the previous page):

1. Identify Risk Management Principles

It is necessary to identify one or more risk management principles that will form the basis of how the entity approaches its risk management processes. The alignment with risk management principles must support the entity's policies and standards for risk management objectives.

Common risk frameworks include:

- NIST SP 800-37
- ISO 31010
- COSO 2019
- OMB A-123

2. Identify, Implement & Document Critical Dependencies.

This is a multi-step process that involves identifying, implementing and documenting the critical dependencies that are necessary to legitimately identify, assess and manage risk:

2A. Risk Management Dependencies

It is vitally important to establish the fundamental risk management dependencies. These need to be standardized entity-wide or the entity will be hampered by conflicting definitions and expectations:

- Define the "acceptable risk" threshold for your entity.
- Define risk occurrence likelihoods.
- Define risk impact effects.
- Define risk levels.
- Define the various levels of entity management who can "sign off" on risk levels.
- Establish a Plan of Action & Milestones (**POA&M**), risk register or some other method to track risks from identification through remediation.

2B. Technology Dependencies

In order to support risk management processes, it is necessary to establish the technology dependencies that affect risk management decisions:

- Maintain accurate and current hardware and software inventories.
- Maintain accurate and current network diagrams.
- Maintain accurate and current Data Flow Diagrams (**DFD**).
- Document the technology dependencies that affect operations (e.g., supporting systems, applications and services).
- Consistent application of security and privacy controls across the entity.
- Situational awareness of technology-related across the entity (e.g., vulnerability scanning & patch management levels).

2C. Business Dependencies

In order to support risk management processes, it is necessary to establish the business dependencies that affect risk management decisions:

- A data classification scheme needs to exist that is consistent across the entity, including an understanding of what constitutes the "crown jewels" of that require enhanced data protection requirements.
- Business leadership needs to dictate the technology support it requires for business operations to function properly. This enables technology and security leadership to define "what right looks like" from a necessary maturity level for security and privacy controls.
- A multi-discipline effort needs to establish and maintain a Supply Chain Risk Management (**SCRM**) program that governs the entity's supply chain. This requires legal, procurement, security, privacy and Line of Business (**LOB**) involvement.
- Policies and standards must be uniformly applied across the entity.
- LOB management needs to ensure its project teams properly document business practices and provide that information to technology, security and privacy personnel in order to ensure a shared understanding of business practices and requirements exists. This information is necessary to build out a System Security & Privacy Plan (**SSPP**).
- Since "the business" owns risk management decisions, the entity needs to ensure that those individuals in roles that make risk management decisions are competent and appropriately trained to make risk-related decisions.

3. Formalize Risk Management Practices

Document a formal **Risk Management Program (RMP)** that supports the entity's policies & standards. The RMP is meant to document the program-level guidance that defines the "who, what, why, when & how" about the entity's specific risk management practices.

4. Establish A Risk Catalog

It is necessary to develop a risk catalog that identifies the possible risk(s) that affect the entity. The use case for the risk catalog is to identify the applicable risk(s) associated with a control deficiency? (*e.g., if the control fails, what risk(s) is the organization exposed to*?). In the context of the SP-RMM, "risk" is defined as:

> *noun A situation where someone or something valued is exposed to danger, harm or loss.*
> *verb To expose someone or something valued to danger, harm or loss.*

In the context of this definition of risk, it is important to define underlying components of this risk definition:

- *Danger: state of possibly suffering harm or injury*
- *Harm: material / physical damage*
- *Loss: destruction, deprivation or inability to use*

With this understanding of what risk is, the **Secure Controls Framework (SCF)** contains a catalog of third-two (32) risks that are directly mapped to each of the SCF's controls.

Risk Grouping	Risk #	Risk
Access Control	R-AC-1	Inability to maintain individual accountability
	R-AC-2	Improper assignment of privileged functions
	R-AC-3	Privilege escalation
	R-AC-4	Unauthorized access
Asset Management	R-AM-1	Lost, damaged or stolen asset(s)
	R-AM-2	Loss of integrity through unauthorized changes
Business Continuity	R-BC-1	Business interruption
	R-BC-2	Data loss / corruption
	R-BC-3	Reduction in productivity
	R-BC-4	Information loss / corruption or system compromise due to technical attack
	R-BC-5	Information loss / corruption or system compromise due to non-technical attack
Exposure	R-EX-1	Loss of revenue
	R-EX-2	Cancelled contract
	R-EX-3	Diminished competitive advantage
	R-EX-4	Diminished reputation
	R-EX-5	Fines and judgements
	R-EX-6	Unmitigated vulnerabilities
	R-EX-7	System compromise
Governance	R-GV-1	Inability to support business processes
	R-GV-2	Incorrect controls scoping
	R-GV-3	Lack of roles & responsibilities
	R-GV-4	Inadequate internal practices
	R-GV-5	Inadequate third-party practices
	R-GV-6	Lack of oversight of internal controls
	R-GV-7	Lack of oversight of third-party controls
	R-GV-8	Illegal content or abusive action

Incident Response	R-IR-1	Inability to investigate / prosecute incidents
	R-IR-2	Improper response to incidents
	R-IR-3	Ineffective remediation actions
	R-IR-4	Expense associated with managing a loss event
Situational Awareness	R-SA-1	Inability to maintain situational awareness
	R-SA-2	Lack of a security-minded workforce

5. Establish A Threat Catalog

It is necessary to develop a threat catalog that identifies possible natural and man-made threats that affect the entity's security & privacy controls. The use case for the threat catalog is to identify applicable natural and man-made threats that affect control execution? (*e.g., if the threat materializes, will the control function as expected?*) In the context of the SP-RMM, "threat" is defined as:

> *noun A person or thing likely to cause damage or danger.*
> *verb To indicate impending damage or danger.*

This threat catalog is sorted by natural and man-made threats:

Threat Grouping	Threat #	Threat
Natural Threat	NT-1	Drought & Water Shortage
	NT-2	Earthquakes
	NT-3	Fire & Wildfires
	NT-4	Floods
	NT-5	Hurricanes & Tropical Storms
	NT-6	Landslides & Debris Flow
	NT-7	Pandemic (Disease) Outbreaks
	NT-8	Severe Weather
	NT-9	Space Weather
	NT-10	Thunderstorms & Lightning
	NT-11	Tornadoes
	NT-12	Tsunamis
	NT-13	Volcanoes
	NT-14	Winter Storms & Extreme Cold
Man-Made Threat	MT-1	Civil or Political Unrest
	MT-2	Hacking & Other Cybersecurity Crimes
	MT-3	Hazardous Materials Emergencies
	MT-4	Nuclear, Biological and Chemical (**NBC**) Weapons
	MT-5	Physical Crime
	MT-6	Terrorism & Armed Attacks
	MT-7	Utility Service Disruption
	MT-8	Dysfunctional Management Practices

6. Establish A Controls Catalog

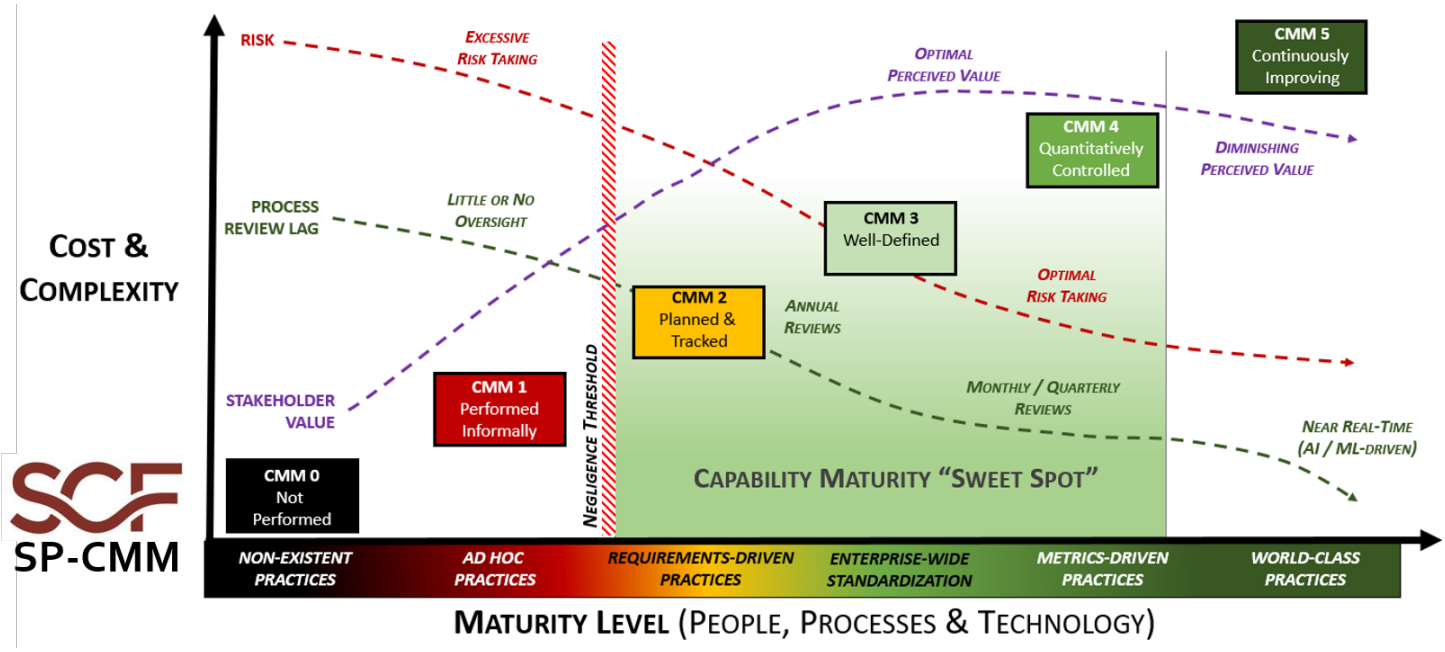
It is necessary to develop a catalog of security and privacy controls that addresses the entity's applicable statutory, regulatory and contractual obligations. Risks must map to the entity's security & privacy controls. Ideally, the controls are weighted since not all security & privacy controls are equal.

Note: The SCF has built-In Control Weighting Values [1-10], a maturity model and the SCF controls written in question format.

7. Define Capability Maturity Model (CMM) Targets

It is necessary for an entity to define "what right looks like" for the level of maturity it expects for deployed security and privacy controls. This is generally defined by aligning with a Capability Maturity Model (**CMM**). While there are several to choose from, the SCF's **Security & Privacy Capability Maturity Model (SP-CMM)** contains control-level criteria for each of the levels of the maturity model.

Maturity model criteria should be used by the organization as the benchmark to evaluate security and privacy controls.



8. Perform Risk Assessments

With the previous steps addressed, an assessor will leverage those deliverables (e.g., Risk Management Program (**RMP**), threat catalog, risk catalog, controls catalogs, etc.) to implement a functional capability to assess risk across the entity. That documented assessment criteria from the previous steps exists to guide the assessor when performing risk assessments.

Assessing risks in the context of the SP-RMM applies to various assessment scenarios:

- Cybersecurity Risk Assessment
- Third-Party Risk Assessment
- Data Protection Impact Assessment (**DPIA**)
- Business Impact Assessment (**BIA**)
- Privacy Impact Assessment (**PIA**)

9. Establish The Context For Assessing Risks

Now that a methodology exists to assess risk, it is necessary for the assessor to establish the context of the Security & Privacy Risk Environment (**SPRE**). The SPRE is the overall operating environment that is in scope for the risk assessment. This is where the threats, risks and vulnerabilities affect the entity's protection measures.

An assessor can generally find this information in a well-documented System Security & Privacy Plan (**SSPP**). If the scoping is incorrect, the context will likely also be incorrect, which can lead to a misguided and inaccurate risk assessment.

10. Controls Gap Assessment

Based on the applicable statutory, regulatory and contractual obligations that impact the SPRE, the entity is expected to have an applicable set of controls to cover those needs. That set of controls identifies the in-scope requirements that must be evaluated to determine what risk exists. This is generally considered to be a "gap assessment" where the assessor:

- Evaluates those controls based on the entity's THREAT CATALOG to identify current or potential control deficiencies; and
- Utilize the RISK CATALOG to identify the applicable risks, based on the identified control deficiencies.

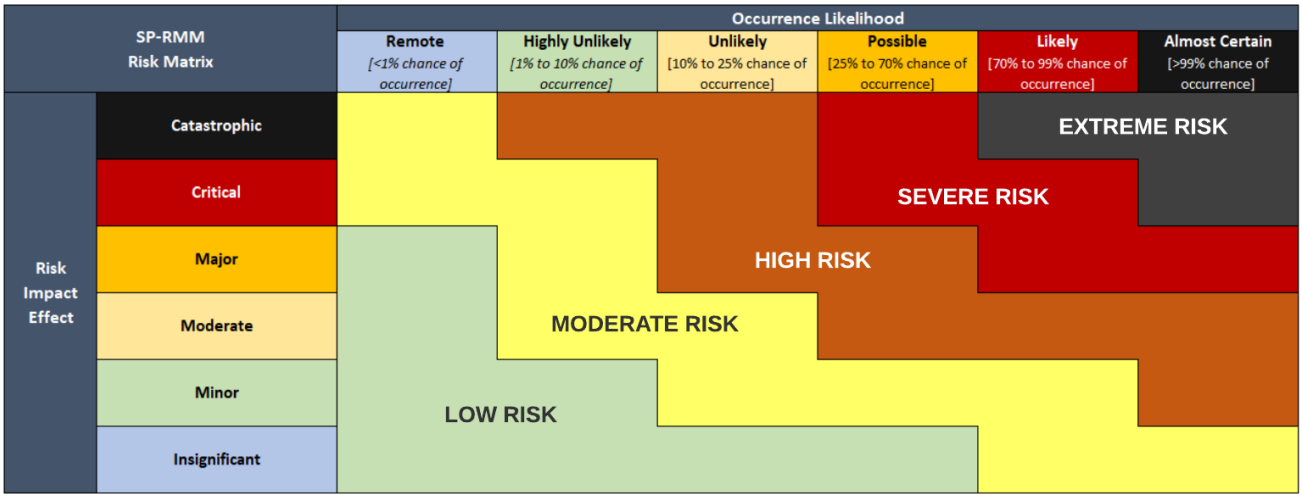
11. Assess Risks

When the control deficiencies are identified, the assessor must utilize an entity-accepted method to assess the risk in the most objective method possible. Methods for assessing a control for deficiencies is generally defined as either:

- Qualitative;
- Semi-Qualitative; or
- Quantitative

In most cases, it is not feasible to have an entirely quantitative assessment, so assessments should be expected to include semi-qualitative or qualitative aspects.

There are multiple methods to actually assess and calculate risk. The SP-RMM leverages work done in this area by **ComplianceForge's Risk Management Program (RMP)** to simplify risk management practices.



12. Determine Risk

At the end of the day, risk needs to be understandable. This is generally why risk is bucketed into a set of pre-defined categories. The SP-RMM leverages the following categories of risk, based on the **ComplianceForge RMP**:

- Low
- Moderate
- High
- Severe
- Extreme

Before a risk report can be documented, it is very important to clarify if the results of the assessment are "inherent risk" or "residual risk" since those have entirely different meanings and implications. Some people want to see both inherent and residual risk, while some people just want to be presented with residual risk. That is why it is important to understand what story the risk scores tell:

- **INHERENT RISK**: The Occurrence Likelihood (**OL**), in combination with the Impact Effect (**IE**) will provide the "inherent risk" score. This is considered a raw or unmitigated risk score. It is important to note that inherent risk does not take into account any control weighting, the maturity of implemented controls or any other mitigating factors.

- **RESIDUAL RISK**: To understand the "residual risk" that takes into account control weighting, the maturity of implemented controls and other mitigating factor, it requires expanding upon inherent risk calculations. To identify the residual risk score, Occurrence Likelihood (**OL**) is calculated by Risk Impact Effect (**IE**), Control Weighting (**CW**), Maturity Level (**ML**) and Mitigating Factors (**MF**).

You can read more about the differences in calculating inherent and residual risk in the CALCULATING RISK: INHERENT RISK VS RESIDUAL RISK section of this document.

13. Prioritize & Document Risks

Once risk has been identified, it is necessary to prioritize and document the identified risk(s). Generally, risk is prioritized by one of the following:

- Emergency;
- Elevated; or
- Standard

Every entity is different in how it documents risk. The following methodologies are commonly used:

- Risk Assessment Report;
- Plan of Action & Milestones (**POA&M**);
- Risk Register; and/or
- System Security & Privacy Plan (**SSPP**)

14. Identify The Appropriate Management Audience

It is an unfortunate and common problem within risk management to run across individuals who are directly impacted by risk and simply say, "I accept the risk" with the intent to "wish away" the risks away so that the project/initiative can proceed without having to first address deficiencies. This is why it is critically important that as part of an entity's program to manage risk that various levels of management are identified with varying authority, each with a pre-described ability to make risk management decisions. This helps prevent low-level managers from recklessly accepting risk that should be reserved for more senior management.

A common tiered structure for risk management decisions includes:

- Line Management
- Senior Management
- Executive Management
- Board of Directors

15. Management Determines Risk Treatment

Risk management is a management decision:

- Cybersecurity and IT generally do not "own" identified risk.
- The ultimate responsibility is on the management structure of the team/department/line of business that "owns" the business process or technology that is in use.

Common risk treatment options include:

- Reduce the risk to an acceptable level
- Avoid the risk
- Transfer the risk to another party
- Accept the risk

Right or wrong, management is ultimately able to decide how risk is to be handled. Where this benefits security, technology and privacy personnel is the "get out of jail" documentation that quality risk assessments and risk management can provide. Instead of executive leadership hanging blame on the CIO or CISO, quality risk management documentation can prove that reasonable steps were taken to identify, assess, report and mitigate risk, which firmly puts the responsibility back on the management team of the team/department/line of business that "owns" the risk.

16. Implement & Document Risk Treatment

When managing risk, it should be kept as simple as possible. Realistically, risk treatment is either "open" or "closed" but it can sometimes be useful to provide more granularity into open items to assist in reporting on risk management activities:

- Open (unacceptable risk)
- Open (acceptable risk)
- Closed

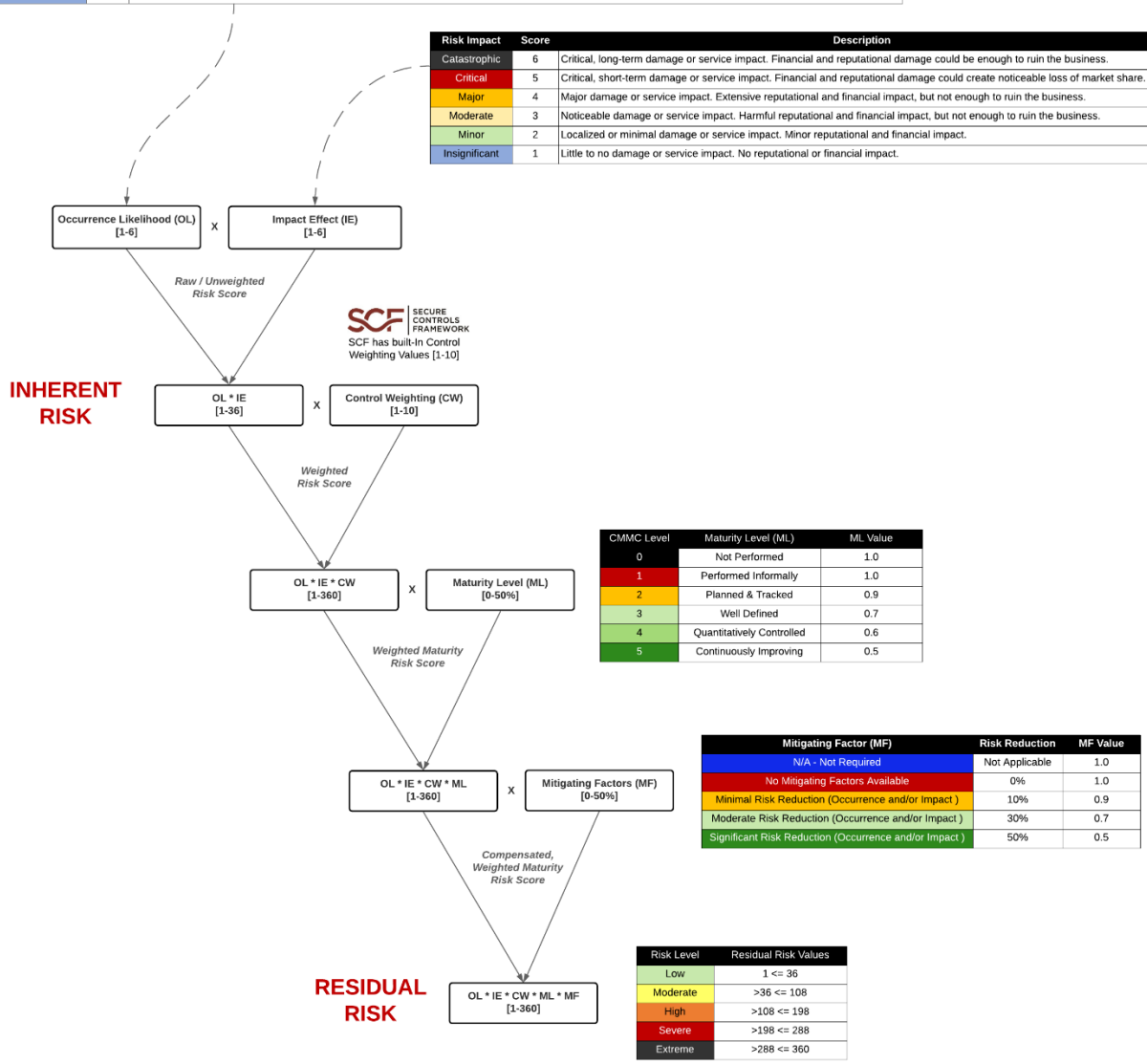
CALCULATING RISK: INHERENT RISK VS RESIDUAL RISK

It is possible to use a straightforward method to calculate risk using SP-RMM. Both Inherent Risk & Residual Risk map into the SP-RMM Risk Matrix (graphic shown below.

- For Inherent Risk, find the cell where Occurrence Likelihood (**OL**) intersects Impact Effect (**IE**) to determine the risk level.
- For Residual Risk, utilize the calculated Residual Risk values to determine the corresponding risk level.

Risk Occurrence	Score	Description
Almost Certain	6	Virtual certainty the event will occur at some time, under normal business conditions, that can be quantified as greater than a 99% chance of occurrence.
Likely	5	Likely to expect the event to occur at some time, under normal business conditions, that can be quantified as between a 70%-99% chance of occurrence.
Possible	4	Reasonable to expect the event could occur at some time, under normal business conditions, that can be quantified as between a 25%-70% chance of occurrence.
Unlikely	3	Unlikely to expect the event to occur at some time, under normal business conditions, that can be quantified as between a 10%-25% chance of occurrence.
Highly Unlikely	2	Highly-unlikely event that can be quantified as between a 1%-10% chance of occurrence.
Remote	1	Theoretically possible. The likelihood of occurring can be quantified as less than a 1% chance of occurrence.

Risk Impact	Score	Description
Catastrophic	6	Critical, long-term damage or service impact. Financial and reputational damage could be enough to ruin the business.
Critical	5	Critical, short-term damage or service impact. Financial and reputational damage could create noticeable loss of market share.
Major	4	Major damage or service impact. Extensive reputational and financial impact, but not enough to ruin the business.
Moderate	3	Noticeable damage or service impact. Harmful reputational and financial impact, but not enough to ruin the business.
Minor	2	Localized or minimal damage or service impact. Minor reputational and financial impact.
Insignificant	1	Little to no damage or service impact. No reputational or financial impact.

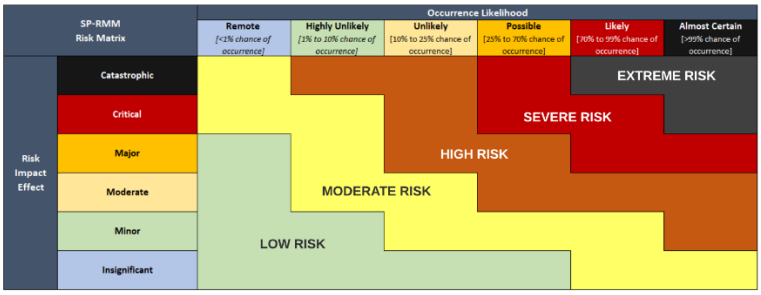


CMMC Level	Maturity Level (ML)	ML Value
0	Not Performed	1.0
1	Performed Informally	1.0
2	Planned & Tracked	0.9
3	Well Defined	0.7
4	Quantitatively Controlled	0.6
5	Continuously Improving	0.5

Mitigating Factor (MF)	Risk Reduction	MF Value
N/A - Not Required	Not Applicable	1.0
No Mitigating Factors Available	0%	1.0
Minimal Risk Reduction (Occurrence and/or Impact)	10%	0.9
Moderate Risk Reduction (Occurrence and/or Impact)	30%	0.7
Significant Risk Reduction (Occurrence and/or Impact)	50%	0.5

Risk Level	Residual Risk Values
Low	1 <= 36
Moderate	>36 <= 108
High	>108 <= 198
Severe	>198 <= 288
Extreme	>288 <= 360

Both **Inherent Risk** & **Residual Risk** map into the **SP-RMM Risk Matrix** (graphic shown below.
- For Inherent Risk, find the cell where Occurrence Likelihood (OL) intersects Impact Effect (IE) to determine the risk level.
- For Residual Risk, utilize the calculated Residual Risk values (see chart above) to determine the corresponding risk level.



Step 1: Calculate The Inherent Risk

To determine the inherent risk, calculate the Occurrent Likelihood (**OL**) by the Impact Effect (**IE**).

Step 2: Account For Control Weighting

Not all security and privacy controls are equal, so it is important to apply weighting to the importance of controls. The SCF contains pre-defined control weightings that can be edited for an entity's unique requirements. This Control Weighting (CW) is multiplied by the inherent risk score from Step 1.

Step 3: Account For Maturity Level Targets

The next step is meant to determine a weighted maturity score that takes control maturity into account. The more mature a control is, the greater the risk should be reduced. Maturity Level (**ML**) is multiplied by the value determined in Step 2.

Step 4: Account For Mitigating Factors To Determine Residual Risk

The final step is to account for Mitigating Factors (**MF**), which can be compensating controls or other process/technology considerations that mitigate risk, specific to the identified threats.

The end calculation to determine residual risk is: **OL * IE * CW * ML * MF**

Leveraging the by **ComplianceForge's Risk Management Program (RMP)** structure, it is straightforward to translate the calculated value of the residual risk score into a user-friendly risk category:

Risk Category	Range
Low	0 <= 36
Moderate	>36 <= 108
High	>108 <= 198
Severe	>198 <= 288
Extreme	>288 <= 360

APPENDIX A. NIST SP 800-171 & CMMC RISK MANAGEMENT CONSIDERATIONS

An immediate need for many organizations is compliance with NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC). The Security & Privacy Risk Management Model (**SP-RMM**) is a tool that can be used to address the following requirements:

CMMC PROCESSES & PRACTICES

These CMMC processes and practices are directly impacted by the SP-RMM:

CMMC V1.02 PROCESSES (LEVELS 1-3)

- RM-MC-ML.2.999. Establish a policy that includes Risk Management (**RM**).
- RM-MC-ML.2.998. Document the CMMC practices to implement the Risk Management (**RM**) policy.
- RM-MC-ML.3.997. Establish, maintain and resource a plan that includes Risk Management (**RM**).

CMMC V1.02 PRACTICES (LEVELS 1-3)

- AT.2.056. Ensure that managers, system administrators and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of those systems.
- RM.2.141. Periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals, resulting from the operation of organizational systems and the associated processing, storage or transmission of CUI.
- RM.3.144. Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources and risk measurement criteria.
- RM.2.143. Remediate vulnerabilities in accordance with risk assessments.
- RM.3.146. Develop and implement risk mitigation plans.
- CA.2.159. Develop and implement plans of action (e.g., POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- CA.3.161. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

NIST SP 800-171 CONTROLS

These NIST SP 800-171 controls are directly impacted by the SP-RMM:

- 3.11.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
- 3.11.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
- 3.11.3. Remediate vulnerabilities in accordance with risk assessments.
- 3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
- 3.12.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- 3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

APPENDIX B. DOCUMENTATION TO SUPPORT RISK MANAGEMENT PRACTICES

RISK MANAGEMENT PROGRAM (RMP)

ComplianceForge developed its Risk Management Program (RMP) as a way to document risk management practices at the strategic, operational and tactical levels. All organizations have a need to manage risk. Most organizations are compelled to management risk and these requirements come from a broad range of statutory, regulatory and contractual origins. Regardless of your industry, requirements to manage cybersecurity risk exist and failing to manage risk could leave your organization exposed to liabilities from non-compliance:

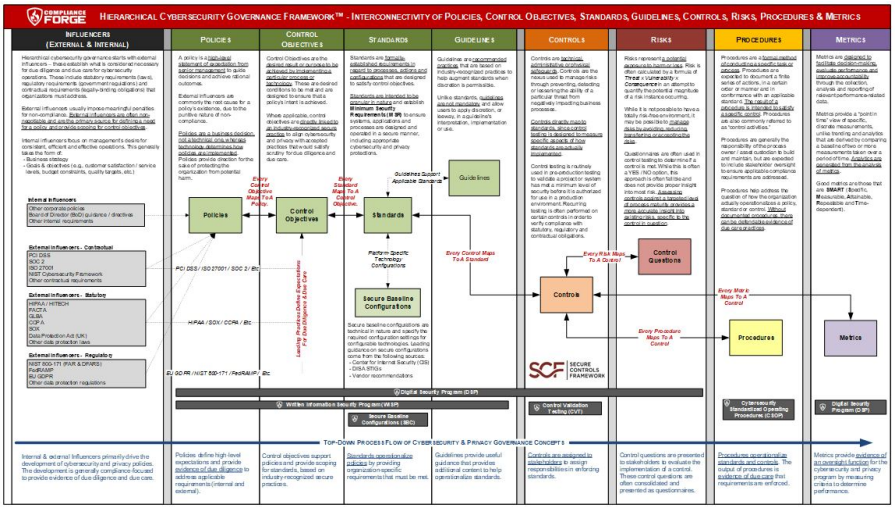
- NIST SP 800-171 & CMMC. Protecting Controlled Unclassified Information (**CUI**) in Nonfederal Information Systems and Organizations – Multiple sections of NIST SP 800-171 & CMMC requires risk to be periodically assessed (see Appendix A for more information on this).
- Federal Trade Commission (**FTC**) Act. 15 U.S. Code § 45 deems unfair or deceptive acts or practices in or affecting commerce to be unlawful - poor security practices are covered under this requirement and not managing cybersecurity risk is an indication of poor security practices.
- Payment Card Industry Data Security Standard (**PCI DSS**). Section#12.2 requires companies to perform a formal risk assessment.
- Health Insurance Portability and Accountability Act (**HIPAA**). Security Rule (Section 45 C.F.R. §§ 164.302 – 318) requires companies to conduct an accurate & thorough assessment of potential risks.
- Gramm-Leach-Bliley Act (**GLBA**). Safeguard Rule requires company to identify and assess risks to customer information.
- Massachusetts MA 201 CMR 17.00. Section# 17.03(2)(b) requires companies to "identify & assess" reasonably-foreseeable internal and external risks.
- Oregon Identity Theft Protection Act. Section 646A.622(2)(d)(B)(ii) requires companies to assess risks in information processing, transmission & storage.
- Vendor Contracts. It is increasingly common for vendors, partners and subcontractors to be contractually-bound to perform recurring risk assessments. Not having a risk management program could lead to breach of contract or losing a bid.

SUPPORTING POLICIES, STANDARDS & PROCEDURES

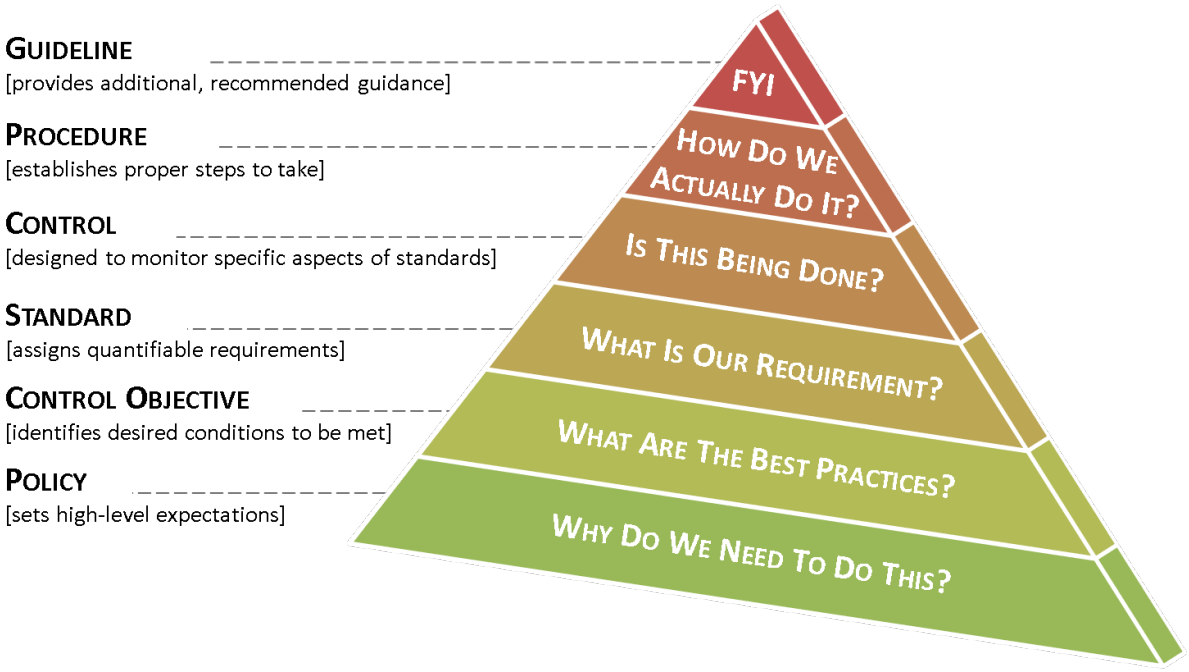
The purpose of a company's cybersecurity & privacy documentation is to prescribe a comprehensive framework for:

- Creating a clearly articulated approach to how your company handles cybersecurity & privacy.
- Protecting the confidentiality, integrity, availability and safety of data and systems on your network.
- Providing guidance to help ensure the effectiveness of cybersecurity and 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 and privacy risks.

When that is all laid out properly, your company's cybersecurity and privacy documentation should flow like the diagram below depicts, where your organization's cybersecurity and privacy policies are linked all the way down to metrics:
http://examples.complianceforge.com/ComplianceForge%20Hierarchical%20Cybersecurity%20Governance%20Framework.pdf



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 cybersecurity documentation build off each other to make a cohesive approach to addressing a requirement:



CYBERSECURITY DOCUMENTATION COMPONENTS

Cybersecurity documentation is comprised of six (6) main parts:

(1) Core policy that establishes management's intent;
(2) Control objective that identifies leading practices;
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(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.