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

Version 2023.1

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:

1. Reduce the risk to an acceptable level;
2. Avoid the risk;
3. Transfer the risk to another party; or
4. 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.

Fundamentally, risk management requires educating stakeholders for situational awareness and decision-making purposes. Reporting risk can be summarized by explaining the "health" of the cybersecurity and privacy program as to how the assessed controls provide assurance that the organization's stated risk tolerance is or is not achieved. This can be categorized according to one of the following risk determinations

1. Conforms;
2. Significant Deficiency; or
3. Material Weakness

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).

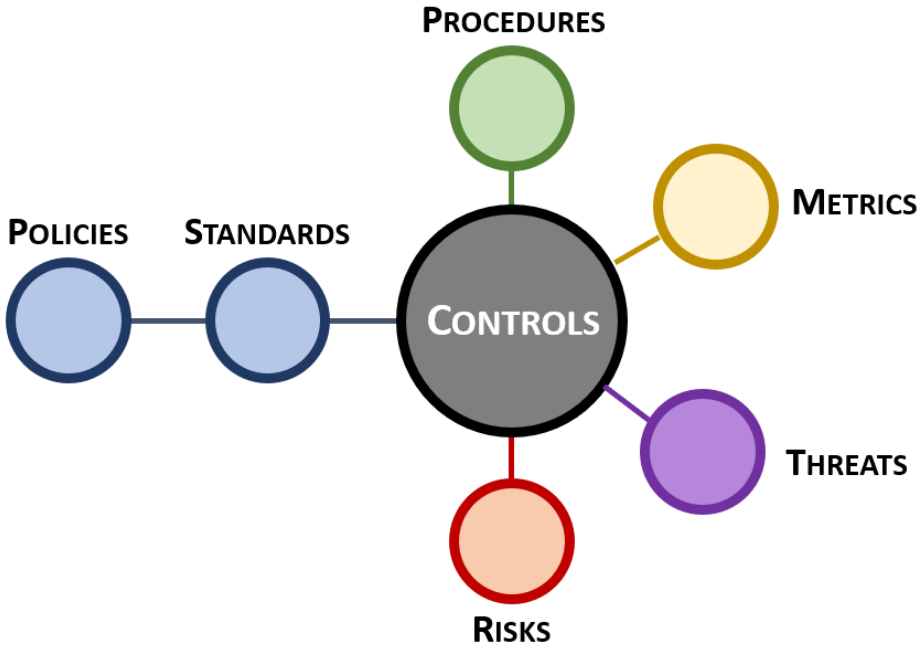
RISKS & THREATS DO NOT EXIST IN A VACUUM

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.



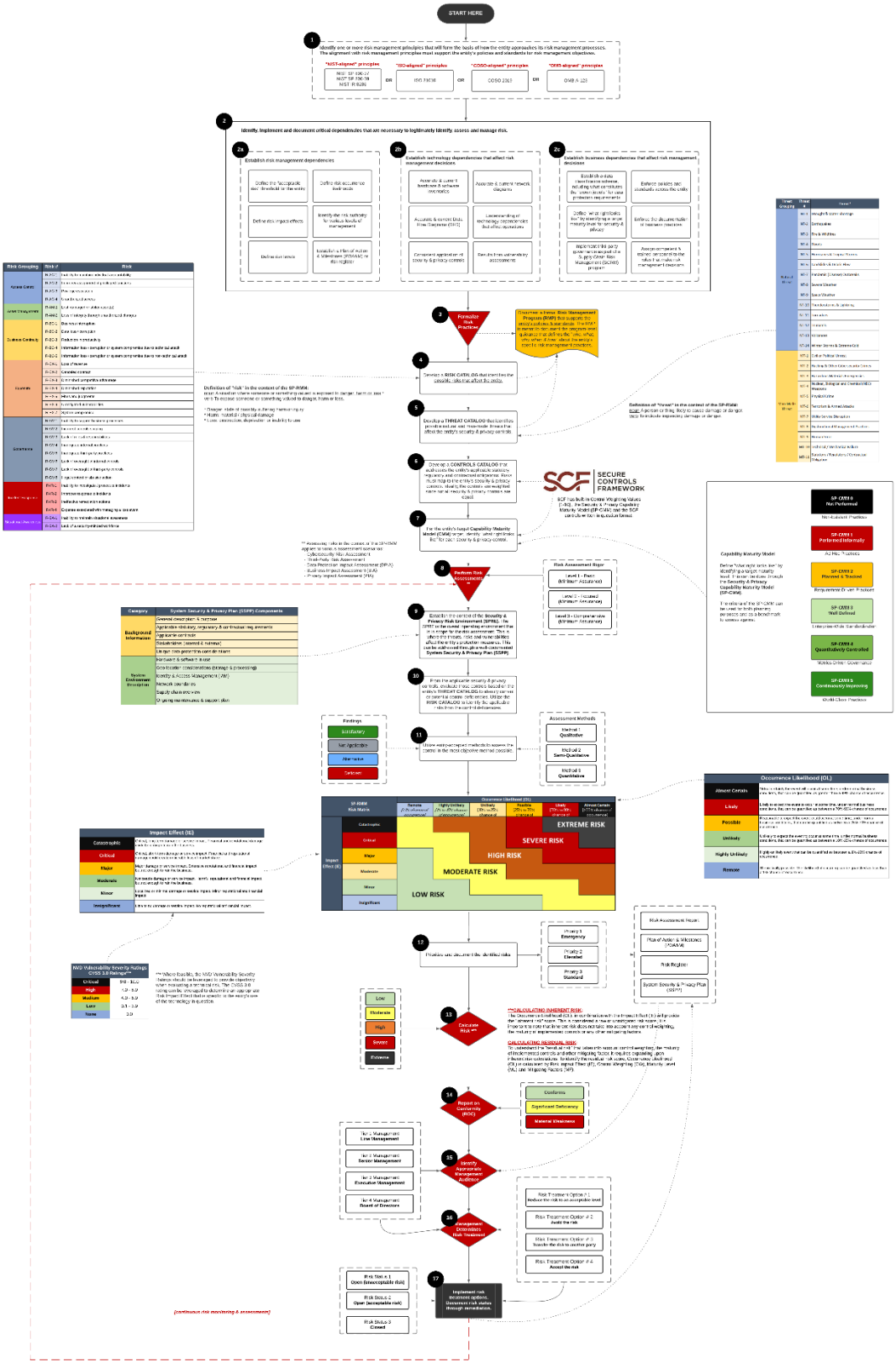
In risk management, the old adage is applicable that "the path to hell is paved with good intentions." Often, risk management personnel are tasked with creating risk assessments and questions to ask without having a centralized set of organization-wide cybersecurity and privacy controls to work from. 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 dependencies need to be standardized entity-wide or the organization will be hampered by conflicting definitions and expectations:

- Define the “acceptable risk” threshold for your entity.
- Define risk Occurrence Likelihood (**OL**).
- Define risk Impact Effect (**IE**).
- 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 organization.
- Situational awareness of technology-related across the organization (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 organization, 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 organization’s supply chain. This requires legal, procurement, security, privacy and Line of Business (**LOB**) involvement.
- Policies and standards must be uniformly applied across the organization.
- 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 LOB “owns” risk management decisions, the organization 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:

- Reference the most appropriate industry frameworks to provide a comprehensive and holistic approach to identifying, managing and remediating risks;
- Incorporate both security and privacy concepts in all stages of asset and data lifecycles; and
- Document the organization's program-level guidance that defines the "who, what, why, when & how" about the organization'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 thirty-three (33) risks that are directly mapped to each of the SCF's controls.

Risk Grouping	Risk #	Risk Note - Some of these risks may indicate a deficiency that could be considered a failure to meet "reasonable security practices"	Description of Possible Risk Due To Control Deficiency IF THE CONTROL FAILS, RISK THAT THE ORGANIZATION IS EXPOSED TO IS:
Access Control	R-AC-1	Inability to maintain individual accountability	The inability to maintain accountability (e.g., asset ownership, non-repudiation of actions or inactions, etc.).
	R-AC-2	Improper assignment of privileged functions	The inability to implement least privileges (e.g., Role-Based Access Control (RBAC), Privileged Account Management (PAM), etc.).
	R-AC-3	Privilege escalation	The inability to restrict access to privileged functions.
	R-AC-4	Unauthorized access	The inability to restrict access to only authorized individuals, groups or services.
Asset Management	R-AM-1	Lost, damaged or stolen asset(s)	Lost, damaged or stolen assets.
	R-AM-2	Loss of integrity through unauthorized changes	Unauthorized changes that corrupt the integrity of the system / application / service.
	R-AM-3	Emergent properties and/or unintended consequences	Emergent properties and/or unintended consequences from Artificial Intelligence & Autonomous Technologies (AAT).
Business Continuity	R-BC-1	Business interruption	Increased latency, or a service outage, that negatively impact business operations.
	R-BC-2	Data loss / corruption	The inability to maintain the confidentiality of the data (compromise) or prevent data corruption (loss).
	R-BC-3	Reduction in productivity	Diminished user productivity.

	R-BC-4	Information loss / corruption or system compromise due to technical attack	A technical attack that compromises data, systems, applications or services (e.g., malware, phishing, hacking, etc.).
	R-BC-5	Information loss / corruption or system compromise due to non-technical attack	A non-technical attack that compromises data, systems, applications or services (e.g., social engineering, sabotage, etc.).
Exposure	R-EX-1	Loss of revenue	A negatively impact on the ability to generate revenue (e.g., a loss of clients or an inability to generate future revenue).
	R-EX-2	Cancelled contract	A cancelled contract with a client or other entity for cause (e.g., failure to fulfill obligations for secure practices).
	R-EX-3	Diminished competitive advantage	Diminished competitive advantage (e.g., lose market share, internal dysfunction, etc.).
	R-EX-4	Diminished reputation	Diminished brand value (e.g., tarnished reputation).
	R-EX-5	Fines and judgements	Financial damages due to fines and/or judgements from statutory / regulatory / contractual non-compliance.
	R-EX-6	Unmitigated vulnerabilities	Unmitigated technical vulnerabilities that lack compensating controls or other mitigation actions.
	R-EX-7	System compromise	A compromise of a system, application or service that affects confidentiality, integrity, availability and/or safety.
Governance	R-GV-1	Inability to support business processes	Insufficient cybersecurity and/or privacy practices that cannot securely support the organization's technologies & processes.
	R-GV-2	Incorrect controls scoping	Missing or incorrect cybersecurity and/or privacy controls due to incorrect or inadequate control scoping practices.
	R-GV-3	Lack of roles & responsibilities	Insufficient cybersecurity and/or privacy roles & responsibilities that cannot securely support the organization's technologies & processes.
	R-GV-4	Inadequate internal practices	Insufficient cybersecurity and/or privacy practices that can securely support the organization's technologies & processes.
	R-GV-5	Inadequate third-party practices	Insufficient Cybersecurity Supply Chain Risk Management (C-SCRM) practices that cannot securely support the organization's technologies & processes.
	R-GV-6	Lack of oversight of internal controls	The inability to demonstrate appropriate evidence of due diligence and due care in overseeing the organization's internal cybersecurity and/or privacy controls.
	R-GV-7	Lack of oversight of third-party controls	The inability to demonstrate appropriate evidence of due diligence and due care in overseeing third-party cybersecurity and/or privacy controls.
	R-GV-8	Illegal content or abusive action	Disruptive content or actions that negatively affect business operations (e.g., abusive content, harmful speech, threats of violence, illegal content, etc.).
Incident Response	R-IR-1	Inability to investigate / prosecute incidents	Insufficient incident response practices that prevent the organization from investigating and/or prosecuting incidents (e.g., chain of custody corruption, available sources of evidence, etc.).
	R-IR-2	Improper response to incidents	The inability to appropriately respond to incidents in a timely manner.
	R-IR-3	Ineffective remediation actions	The inability to ensure incident response actions were correct and/or effective.

	R-IR-4	Expense associated with managing a loss event	Financial repercussions from responding to an incident or loss.
Situational Awareness	R-SA-1	Inability to maintain situational awareness	The inability to detect cybersecurity and/or privacy incidents (e.g., a lack of situational awareness).
	R-SA-2	Lack of a security-minded workforce	The inability to appropriately educate and train personnel to foster 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:

5A. Natural Threats

Natural threats are caused by environmental phenomena that have the potential to impact individuals, processes, organizations or society, as a whole. The SP-RMM leverages a catalog of fourteen (14) natural threats:

Threat #	Threat	Threat Description
NT-1	Drought & Water Shortage	Regardless of geographic location, periods of reduced rainfall are expected. For non-agricultural industries, drought may not be impactful to operations until it reaches the extent of water rationing.
NT-2	Earthquakes	Earthquakes are sudden rolling or shaking events caused by movement under the earth's surface. Although earthquakes usually last less than one minute, the scope of devastation can be widespread and have long-lasting impact.
NT-3	Fire & Wildfires	Regardless of geographic location or even building material, fire is a concern for every business. When thinking of a fire in a building, envision a total loss to all technology hardware, including backup tapes, and all paper files being consumed in the fire.
NT-4	Floods	Flooding is the most common of natural hazards and requires an understanding of the local environment, including floodplains and the frequency of flooding events. Location of critical technologies should be considered (e.g., server room is in the basement or first floor of the facility).
NT-5	Hurricanes & Tropical Storms	Hurricanes and tropical storms are among the most powerful natural disasters because of their size and destructive potential. In addition to high winds, regional flooding and infrastructure damage should be considered when assessing hurricanes and tropical storms.
NT-6	Landslides & Debris Flow	Landslides occur throughout the world and can be caused by a variety of factors including earthquakes, storms, volcanic eruptions, fire, and by human modification of land. Landslides can occur quickly, often with little notice. Location of critical technologies should be considered (e.g., server room is in the basement or first floor of the facility).

NT-7	Pandemic (Disease) Outbreaks	Due to the wide variety of possible scenarios, consideration should be given both to the magnitude of what can reasonably happen during a pandemic outbreak (e.g., COVID-19, Influenza, SARS, Ebola, etc.) and what actions the business can be taken to help lessen the impact of a pandemic on operations.
NT-8	Severe Weather	Severe weather is a broad category of meteorological events that include events that range from damaging winds to hail.
NT-9	Space Weather	Space weather includes natural events in space that can affect the near-earth environment and satellites. Most commonly, this is associated with solar flares from the Sun, so an understanding of how solar flares may impact the business is of critical importance in assessing this threat.
NT-10	Thunderstorms & Lightning	Thunderstorms are most prevalent in the spring and summer months and generally occur during the afternoon and evening hours, but they can occur year-round and at all hours. Many hazardous weather events are associated with thunderstorms. Under the right conditions, rainfall from thunderstorms causes flash flooding and lightning is responsible for equipment damage, fires and fatalities.
NT-11	Tornadoes	Tornadoes occur in many parts of the world, including the US, Australia, Europe, Africa, Asia, and South America. Tornadoes can happen at any time of year and occur at any time of day or night, but most tornadoes occur between 4–9 p.m. Tornadoes (with winds up to about 300 mph) can destroy all but the best-built man-made structures.
NT-12	Tsunamis	All tsunamis are potentially dangerous, even though they may not damage every coastline they strike. A tsunami can strike anywhere along most of the US coastline. The most destructive tsunamis have occurred along the coasts of California, Oregon, Washington, Alaska and Hawaii.
NT-13	Volcanoes	While volcanoes are geographically fixed objects, volcanic fallout can have significant downwind impacts for thousands of miles. Far outside of the blast zone, volcanoes can significantly damage or degrade transportation systems and also cause electrical grids to fail.
NT-14	Winter Storms & Extreme Cold	Winter storms is a broad category of meteorological events that include events that range from ice storms, to heavy snowfall, to unseasonably (e.g., record breaking) cold temperatures. Winter storms can significantly impact business operations and transportation systems over a wide geographic region.

5B. MANMADE THREATS

Manmade threats are caused by an element of human intent, negligence or error, or threat of violence that have the potential to impact individuals, processes, organizations or society, as a whole. The SP-RMM leverages a catalog of eleven (11) manmade threats:

Threat #	Threat	Threat Description
MT-1	Civil or Political Unrest	Civil or political unrest can be singular or wide-spread events that can be unexpected and unpredictable. These events can occur anywhere, at any time.
MT-2	Hacking & Other Cybersecurity Crimes	Unlike physical threats that prompt immediate action (e.g., "stop, drop, and roll" in the event of a fire), cyber incidents are often difficult to identify as the incident is occurring. Detection generally occurs after the incident has occurred, with the exception of "denial of service" attacks. The spectrum of cybersecurity risks is limitless and threats can have wide-ranging effects on the individual, organizational, geographic, and national levels.

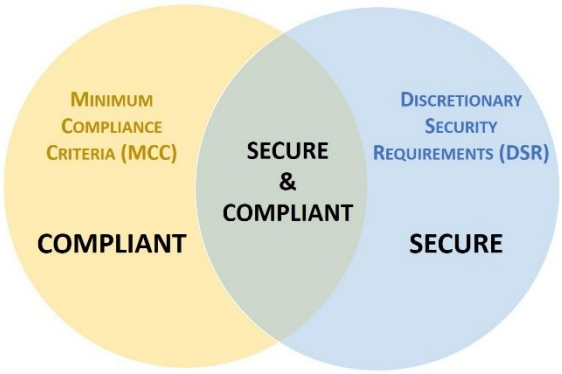
MT-3	Hazardous Materials Emergencies	Hazardous materials emergencies are focused on accidental disasters that occur in industrialized nations. These incidents can range from industrial chemical spills to groundwater contamination.
MT-4	Nuclear, Biological and Chemical (NBC) Weapons	The use of NBC weapons are in the possible arsenals of international terrorists and it must be a consideration. Terrorist use of a “dirty bomb” — is considered far more likely than use of a traditional nuclear explosive device. This may be a combination a conventional explosive device with radioactive / chemical / biological material and be designed to scatter lethal and sub-lethal amounts of material over a wide area.
MT-5	Physical Crime	Physical crime includes "traditional" crimes of opportunity. These incidents can range from theft, to vandalism, riots, looting, arson and other forms of criminal activities.
MT-6	Terrorism & Armed Attacks	Armed attacks, regardless of the motivation of the attacker, can impact a businesses. Scenarios can range from single actors (e.g., "disgruntled" employee) all the way to a coordinated terrorist attack by multiple assailants. These incidents can range from the use of blade weapons (e.g., knives), blunt objects (e.g., clubs), to firearms and explosives.
MT-7	Utility Service Disruption	Utility service disruptions are focused on the sustained loss of electricity, Internet, natural gas, water, and/or sanitation services. These incidents can have a variety of causes but directly impact the fulfillment of utility services that your business needs to operate.
MT-8	Dysfunctional Management Practices	Dysfunctional management practices are a manmade threat that expose an organization to significant risk. The threat stems from the inability of weak, ineffective and/or incompetent management to (1) make a risk-based decision and (2) support that decision. The resulting risk manifests due (1) an absence of a required control or (2) a control deficiency.
MT-9	Human Error	Human error is a broad category that includes non-malicious actions that are unexpected and unpredictable by humans. These incidents can range from misconfigurations to misunderstandings or other unintentional accidents.
MT-10	Technical / Mechanical Failure	Technical /mechanical failure is a broad category that includes non-malicious failure due to a defect in the technology, materials or workmanship. Technical / mechanical failures are unexpected and unpredictable, even when routine and preventative maintenance is performed. These incidents can range from malfunctions to reliability concerns to catastrophic damage.
MT-11	Statutory / Regulatory / Contractual Obligation	Laws, regulations and/or contractual obligations that directly or indirectly weaken an organization's security & privacy controls. This includes hostile nation states that leverage statutory and/or regulatory means for economic or political espionage and/or cyberwarfare activities.
MT-12	Redundant, Obsolete/Outdated, Toxic or Trivial (ROT) Data	Redundant, Obsolete/Outdated, Toxic or Trivial (ROT) data is information an organization utilizes for business processes even though the data is untrustworthy, due to the data's currency, accuracy, integrity and/or applicability.
MT-13	Artificial Intelligence & Autonomous Technologies (AAT)	Artificial Intelligence & Autonomous Technologies (AAT) is a broad category that ranges from non-malicious failure due to a defect in the algorithm to emergent properties or unintended consequences. AAT failures can be due to hardware failures, inherent biases or other flaws in the underlying algorithm. These incidents can range from malfunctions, to reliability concerns to catastrophic damage (including loss of life).

6. Establish A Controls Catalog

It is necessary to develop a catalog of security and privacy controls that addresses the organization's applicable statutory, regulatory and contractual obligations. Risks used by the organization as part of risk analysis processes must map to the organization's existing security & privacy controls. Ideally, the controls are weighted since not all security & privacy controls are equal, in terms of impact or consequence.

To assist in this process, it is helpful for the organization to categorize its applicable controls according to "must have" vs "nice to have" requirements:[1]

- Minimum Compliance Criteria (**MCC**) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- Discretionary Security Requirements (**DSR**) are tied to the organization's risk appetite since DSR are "above and beyond" MCC, where the organization self-identifies additional cybersecurity and data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.

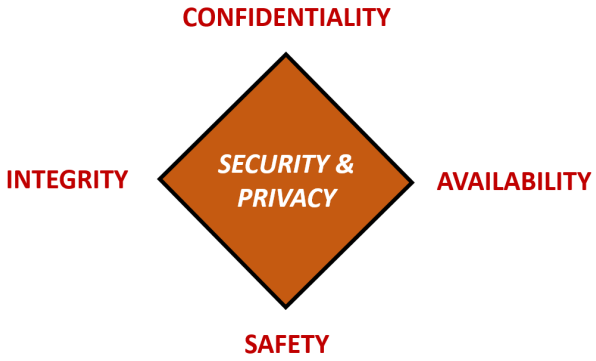


Secure and compliant operations exist when both MCC and DSR are implemented and properly governed:

- MCC are primarily externally-influenced, based on industry, government, state and local regulations. MCC should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCC establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

The combination of MCC and DSR equate to an organization's Minimum Security Requirements (**MSR**), which define the "must have" and "nice to have" requirements for People, Processes, Technology & Data (**PPTD**) in one control set. It defines the Minimum Viable Product (**MVP**) technical and business requirements from a cybersecurity and privacy perspective. In short, the MSR can be considered to be an organization's IT General Controls (**ITGC**), which establish the basic controls that must be applied to systems, applications, services, processes and data throughout the enterprise. ITGC provide the foundation of assurance for an organization's decision makers. ITGC enables an organization's governance function to define how technologies are designed, implemented and operated.

Commensurate with risk, security and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure Confidentiality, Integrity, Availability and Safety (**CIAS**):



- **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.
- **Safety** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

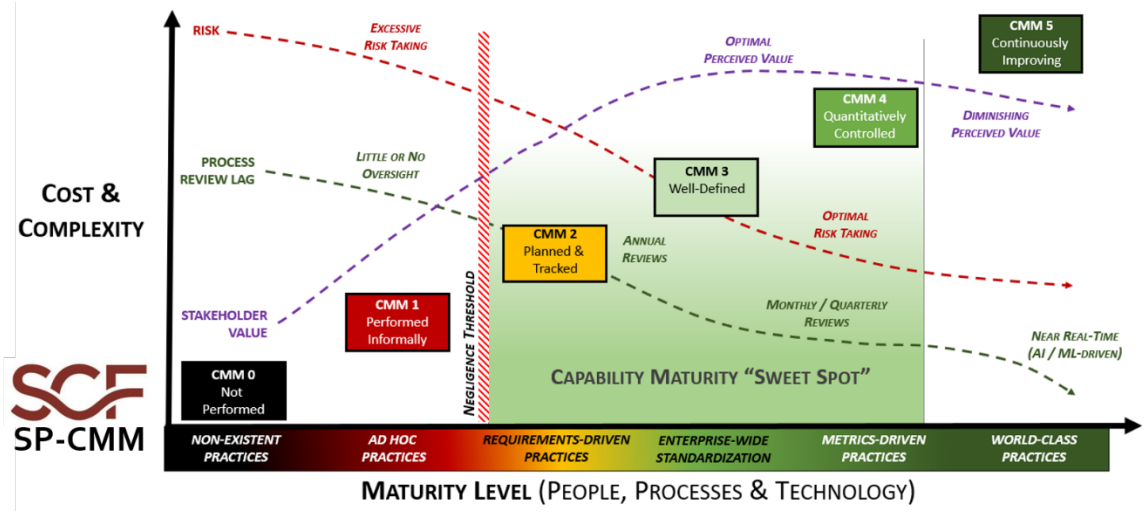
Note: The SCF has built-In Control Weighting Values [1-10], a maturity model and the SCF controls written in question format.

[1] *Integrated Controls Management (ICM) model - http://integrated-controls-management.com/*

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 RMS applies to various assessment scenarios:

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

8A. Risk Assessment Level 1: Basic (Minimum Assurance)

Basic risk assessments provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors.

8B. Risk Assessment Level 2: Focused (Moderate Assurance)

Focused risk assessments provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.

8C. Risk Assessment Level 3: Comprehensive (High Assurance)

Comprehensive risk assessments provide a level of understanding of the security safeguards necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the safeguards.

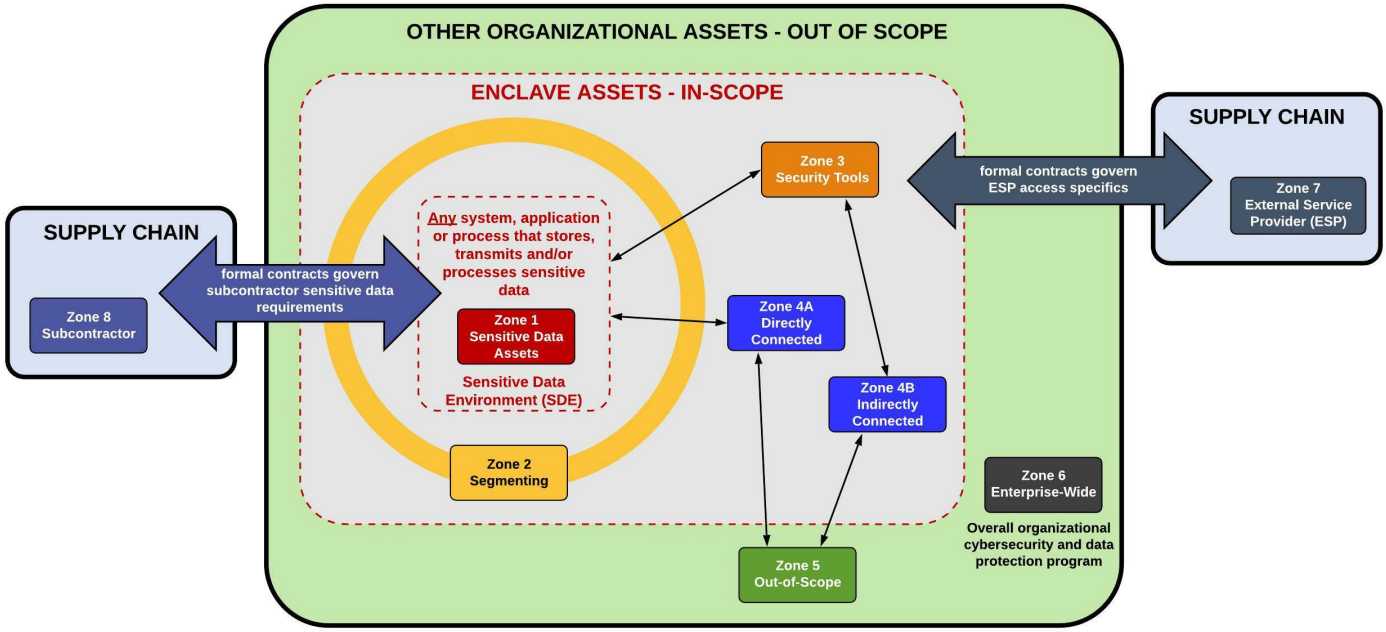
9. Establish The Context For Assessing Risks

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 applicable 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.

SPRE Context	SSPP Component
Background Information	General description & purpose
	Applicable statutory, regulatory & contractual requirements
	Applicable contracts
	Stakeholders (internal & external)
	Unique data protection considerations
System Environment Description	Hardware & software in use
	Geolocation considerations
	Identity & Access Management (IAM)
	Network boundaries
	Supply chain overview
	Ongoing maintenance & support plan

Without specific statutory, regulatory or contractual scoping instructions, the organization should leverage the Unified Scoping Guide (**USG**) as the basis for scoping sensitive and/or regulated data.[2]



[2] *Unified Scoping Guide (USG) - https://www.unified-scoping-guide.com/*

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.

Whenever possible, Assessment Objectives (AOs) need to be used to assess a control. Per the NIT Glossary, an AO is "a set of determination statements that expresses the desired outcome for the assessment of a security control, privacy control, or control enhancement." There may be one or more AOs assigned to a control and all AOs are expected to be satisfied to legitimately be able to conform to the intent of the control.

11. Assess Controls To Determine Findings

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 simplifies risk management practices by utilizing a form of risk matrix that takes Occurrence Likelihood (OL) and Impact Effect (IE) into account to determine the risk categorization.

When a control is assessed, the result is referred to as a finding. Findings are not designed to have a specific "score" associated with the evaluation of a control. Its value is in the subjective status associated with the implementation of the control. These findings are useful for the Report on Conformity (ROC), or whatever you want to call the risk assessment report, to summarize the findings to the organization's management.

The four (4) categories of findings are:

1. Satisfactory
2. Not Applicable
3. Alternative Control
4. Deficient

11A. Satisfactory

Positive finding. Appropriate evidence of due diligence and due care exists to demonstrate the design and/or operation of an organization's cybersecurity and/or data protection control satisfactorily meets all applicable Assessment Objectives (AOs) that determine if the intent of the control is achieved.

11B. Not Applicable

Neutral finding. Appropriate evidence demonstrates the control is not applicable, due to applicable business practices and/or technical implementation.

11C. Alternative Control

Positive finding. Appropriate evidence of due diligence and due care exists to demonstrate the design and/or operation of an organization's cybersecurity and/or data protection control satisfactorily meets all applicable AOs that determine if the intent of the control is achieved.

11D. Deficient

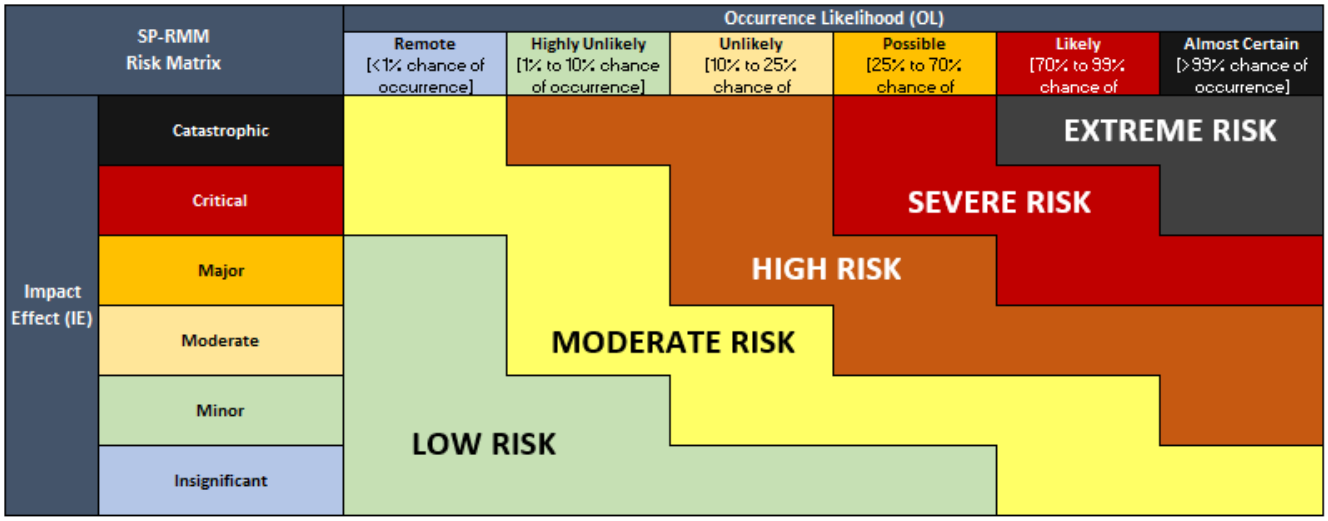
Negative finding. A "deficiency" exists when the design and/or operation of an organization's cybersecurity and/or data protection control fails to meet one of more AO that determine if the intent of the control is achieved.

A deficiency would fail to reasonably prevent or detect a threat in a timely manner.

- A design-related deficiency exists when a control fails to meet the control objective, so even if that control operates as it was

designed, the operation of that control would fail to satisfy one or more AOs.
- An operation-related deficiency exists when a control does not operate as it was designed.

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. Prioritize Identified Deficiencies

Once a deficiency with a control is identified, it is necessary to determine the level of urgency that should be applied to it. Findings need to be categorized by one of the following levels of prioritization:

- Emergency;
- Elevated; or
- Standard.

The organization's risk documentation methodology should utilize one or more of the following options:

- Risk Register
- Plan of Action & Milestones (**POA&M**)
- Risk Assessment Report
- System Security & Privacy Plan (**SSPP**);or
- Another documentation option of your choosing.

13. Calculating Risk

Risk can be calculated at a single control or a summary of multiple controls. The SP-RMM makes it possible to categorize risk into a set of pre-defined levels of risk that result from an intersection of

. The SP-RMM leverages the following categories of risk:

- Low;
- Moderate;
- High;
- Severe; and
- 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, **OL** is calculated by **IE**, Control Weighting (**CW**), Maturity Level (**ML**) and Mitigating Factors (**MF**).

14. Risk Determination: Report on Conformity (ROC)

Risk management requires educating stakeholders for situational awareness and decision-making purposes. There are many options and formats available to report, but this can be considered a Report on Conformity (**ROC**). The reason for this is a risk assessment fundamentally is evaluating if an organization's cybersecurity and privacy practices support its stated risk tolerance.

This approach can be summarized by reporting to the organization's management on the "health" of the assessed controls by one of the following risk determinations:

1. Conforms
2. Significant Deficiency
3. Material Weakness

14A. Conforms

This is a positive outcome and indicates that at a high-level, the organization's cybersecurity and privacy practices conform to its selected cybersecurity and privacy practices. At the control level, there may be one or more deficient controls, but as a whole, the cybersecurity and privacy practices support the organization's stated risk tolerance

It is a statement that the assessed controls conform indicates to the organization's management that sufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance can be achieved.

14B. Significant Deficiency

This is a negative outcome and indicates the organization was unable to demonstrate conformity with its selected cybersecurity and privacy practices, due to systematic problems. Further, this indicates cybersecurity and privacy practices fail to support the organization's stated risk tolerance. This is less severe than a material weakness, but merits executive leadership attention.

It is a statement that the assessed controls have a significant deficiency indicates to the organization's management that insufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance is achieved, due to a systemic problem in the cybersecurity and/or privacy program.

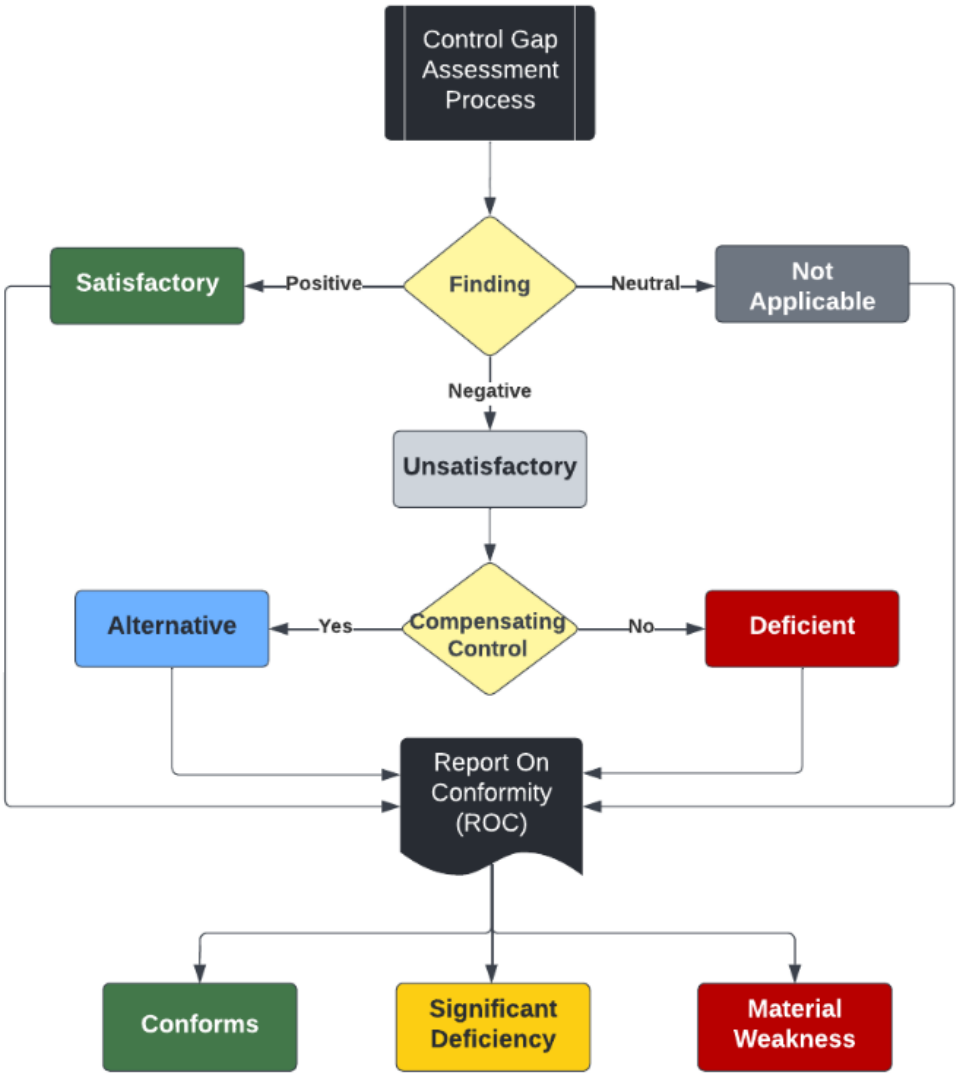
In the context of a significant deficiency, a systemic problem is a consequence of issues inherent in the overall function (e.g., team, department, project, application, service, vendor, etc.), rather than a specific, isolated factor. Systemic errors may require changing the structure, personnel, technology and/or practices to remediate the significant deficiency.

14C. Material Weakness

This is a negative outcome and indicates the organization is unable to demonstrate conformity with its selected cybersecurity and privacy practices, due to deficiencies that make it probable that reasonable-expected threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance.

This indicates cybersecurity and privacy practices fail to support the organization's stated risk tolerance.

A statement that the assessed controls have a material weakness indicates to the organization's management that (1) the cybersecurity and/or privacy program is incapable of successfully performing its stated mission and (2) drastic changes to people, processes and/or technology are necessary to remediate the findings.



15. Identify The Appropriate Management Audience

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; and
- Board of Directors.

the organization's RMP defines the specific risk authority that roles have to make risk management decisions.

16. 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/LOB 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; and
- Accept the risk.

17. 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); and
- Closed.

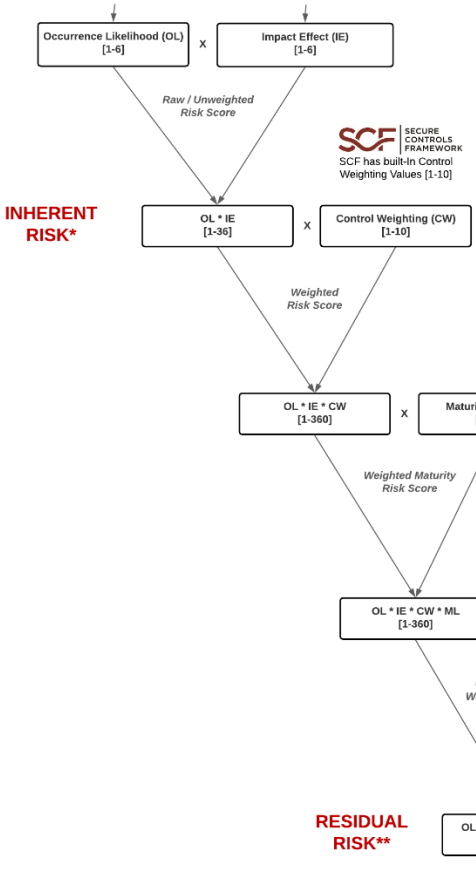
CALCULATING RISK: INHERENT RISK VS RESIDUAL RISK

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.

Occurrence Likelihood (OL)	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.

Impact Effect (IE)	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.



CALCULATING INHERENT RISK:** ***[OL * IE]

The Occurrence Likelihood (OL), in combination with the Impact Effect (IE) will provide the "inherent risk" score.

Note - Inherent risk does not take into account any control weighting, the maturity of implemented controls or any other mitigating factors.

****CALCULATING RESIDUAL RISK:** ***[OL* IE * CW * ML * MF]***

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.

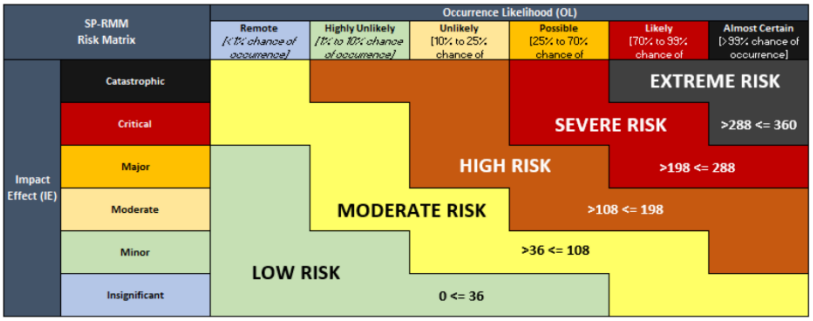
To identify the residual risk score, Occurrence Likelihood (OL) is calculated by Risk Impact Effect (IE), Control Weighting (CW), Maturity Level (ML) and Mitigating Factors (MF).

Maturity Level (ML)	ML Description	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 Impact Reduction (Occurrence and/or Impact)	10%	0.9
Moderate Impact Reduction (Occurrence and/or Impact)	30%	0.7
Significant Impact 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: CYBERSECURITY MATERIALITY & RISK TOLERANCE CONSIDERATIONS

Controls are the nexus of a cybersecurity and privacy program, so it is vitally important to understand how controls should be viewed from a high-level risk management perspective. This brings up the concept of "cybersecurity materiality" as it pertains to the governance of an organization's cybersecurity and privacy controls.

DEFINING CYBERSECURITY MATERIALITY

The Secure Controls Framework (SCF) took the initiative to define cybersecurity materiality and provide examples of risk tolerance levels so that organizations are better equipped to conduct realistic risk management discussions. Specific to cybersecurity and data protection, the SCF defines material weakness as:

> "A deficiency, or a combination of deficiencies, in an organization's cybersecurity and data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance."

In the context of that definition of cybersecurity materiality, it is important to baseline the understanding risk management terminology. According to the PMBOK® Guide:

- Risk Tolerance is the "*specified range of acceptable results*."
- Risk Threshold is the "*level of risk exposure above which risks are addressed and below which risks may be accepted*."
- Risk Appetite is the "*degree of uncertainty an organization or individual is willing to accept in anticipation of a reward*." It is important to note that the risk tolerance and risk appetite are not the same thing. In terms of cybersecurity materiality, risk tolerance matters.

The concept of materiality is important to understand the health of a cybersecurity and data protection program, where a material weakness crosses an organization's risk threshold by making an actual difference that exposes systems, applications, services, personnel, the organization or third-parties to unacceptable risk. Materiality designations can help determine what constitutes reasonable assurance that an organization adheres to its stated risk tolerance.

Assurance is defined as the grounds for confidence that the set of intended security and privacy controls in a system, application or service are effective in their application. Since assurance is relative to a specific set of controls, defects in those controls affect the underlying confidence in the ability of those controls to operate as intended to produce the stated results. Fundamentally, assurance identifies the level of confidence that a stakeholder has that an objective is achieved, that takes into consideration the risks associated with non-conformity (e.g., non-compliance) and the anticipated costs necessary to demonstrate conformity with the specified controls.

When organizations go through some form of certification process, it undergoes a conformity assessment (e.g., ISO 27001, CMMC, SOC 2, PCI DSS, RMF, etc.). Conformity assessments are designed to assure that a particular product, service, or system meets a given level of quality or safety. Instead of a 100% pass criteria, conformity assessments rely on the concept of assurance to establish a risk-based threshold to determine if the intent of the objective(s) has been achieved.

CONTEXT FOR CYBERSECURITY MATERIALITY USAGE

In legal terms, "material" is defined as something that is relevant and significant:[3]

- In a lawsuit, "material evidence" is distinguished from totally irrelevant or of such minor importance that the court will either ignore it, rule it immaterial if objected to, or not allow lengthy testimony upon such a matter.
- A "material breach" of a contract is a valid excuse by the other party not to perform. However, an insignificant divergence from the terms of the contract is not a material breach.

For those in the Governance, Risk Management & Compliance (**GRC**) space, materiality is often relegated to Sarbanes-Oxley Act (**SOX**) compliance. However, the concept of materiality is much broader than SOX and can be applied as part of risk reporting in any type of conformity assessment. Financial-related materiality definitions focus on investor awareness of third-party practices, not inwardly-looking for adherence to an organization's risk tolerance:

- Per the Security and Exchange Commission (**SEC**), information is material "*to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered.*"[4]
- Per the Financial Accounting Standards Board (**FASB**), "*omissions or misstatements of items are material if they could, individually or collectively, influence the economic decisions that users make on this basis of the financial statements.*"[5]

[3] *https://dictionary.law.com/Default.aspx?selected=1223*
[4] *17 C.F.R. § 230.405*
[5] *https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/asb/documents/mtg/1810/2018-10-asb-itema.pdf*

Defining Risk Tolerance

An organization's risk tolerance is influenced by several factors that includes, but is not limited to:

- Statutory, regulatory and contractual compliance obligations
- Adherence to privacy principles for ethical data protection practices
- Organization-specific threats (natural and manmade)
- Expected industry practices
- Pressure from competition
- Executive management preferences

The following three (3) categories establish risk tolerance levels for [Company Name]. These categories range from "low" to "high" risk tolerance and allow for a more granular understanding of risk. Risk tolerance is simplified as being one of the following three levels:

1. Low;
2. Moderate; or
3. High

Low Risk Tolerance

Organizations that would be reasonably-expected to adopt a low risk tolerance generally:

- Provide products and/or services that are necessary for the population to maintain normalcy in daily life;
- Are in a highly-regulated industries with explicit cybersecurity and/or data protection requirements;
- Store, process and/or transmit highly-sensitive/regulated data;
- Are legitimate targets for nation-state actors to disrupt and/or compromise due to the high-value nature of the organization;
- Have strong executive management support for security and privacy practices being part of "business as usual" activities;
- Maintain a high level of capability maturity for preventative cybersecurity controls to implement "defense in depth" protections across the enterprise;
- Have a high level of situational awareness (cybersecurity & physical) that includes its supply chain; and
- Have cyber-related insurance.

Organizations that are reasonably expected to operate with a low risk tolerance include, but are not limited to:

- Critical infrastructure
  - Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.)
  - Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, Cloud Service Providers (CSPs), etc.) (high value)
  - Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.)
- Technology Research & Development (R&D) (high value)
- Healthcare (high value)
- Government institutions
  - Military
  - Law enforcement
  - Judicial system
- Financial services (high value)
- Defense Industrial Base (DIB) contractors (high value)

Moderate Risk Tolerance

Organizations that would be reasonably-expected to adopt a moderate risk tolerance generally:

- Have executive management support for securing sensitive data enclaves;
- Are in a regulated industries that have specific cybersecurity and/or data protection requirements (e.g., CMMC, PCI DSS, SOX, GLBA, RMF, etc.);
- Have "flow down" requirements from customers that require adherence to certain cybersecurity and/or data protection requirements;
- Store, process and/or transmit sensitive/regulated data;
- Are legitimate targets for attackers who wish to financially benefit from stolen information or ransom; and
- Have cyber-related insurance.

Organizations that are reasonably expected to operate with a moderate risk tolerance include, but are not limited to:

- Education (e.g., K-12, colleges, universities, etc.)

    - Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.)
    - Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, etc.)
    - Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.)
- Technology services (e.g., Managed Service Providers (MSPs), Managed Security Service Providers (MSSP), etc.)
- Manufacturing (high value)
- Healthcare
- Defense Industrial Base (DIB) contractors and subcontractors
- Legal services (e.g., law firms)
- Construction (high value)

HIGH RISK TOLERANCE

Organizations that would be reasonably-expected to adopt a high risk tolerance generally:

- Are in an unregulated industry, as it pertains to cybersecurity and/or data protection requirements;
- Do not store, process and/or transmit sensitive/regulated data;
- Lack management support for cybersecurity and privacy governance practices; and
- Do not have cyber-related insurance.

Organizations that may choose to operate with a high risk tolerance include, but are not limited to:

- Restaurants
- Hospitality industry
- Construction
- Manufacturing
- Personal services

APPENDIX B: 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:

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 C: 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:

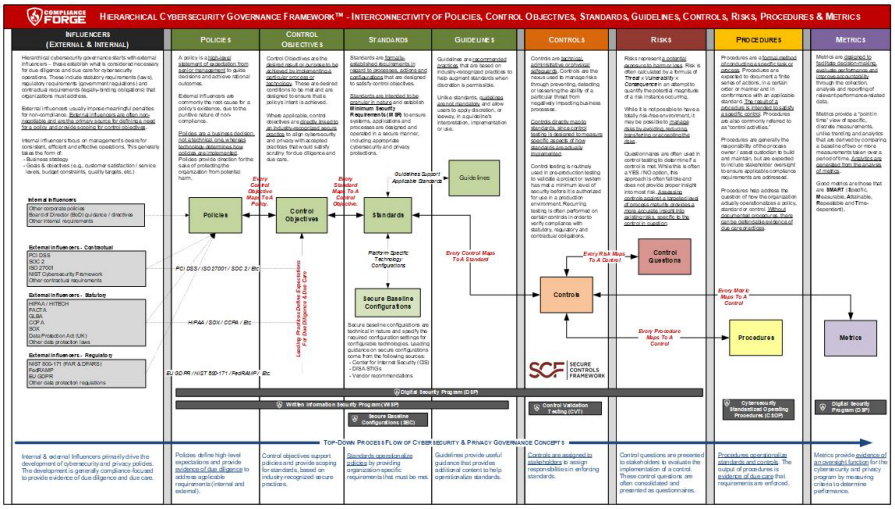
- NIST SP 800-171 & CMMC. Protecting Controlled Unclassified Information (**CUI**) in Nonfederal Information Systems and Organizations – Multiple sections of NIST SP 800-171 & CMMC requires risk to be periodically assessed (see Appendix A for more information on this).
- Federal Trade Commission (**FTC**) 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 five (5) core components:

(1) Policies are established by the organization's corporate leadership establishes "management's intent" for cybersecurity and data protection requirements that are necessary to support the organization's overall strategy and mission;
(2) Control Objectives identify the technical, administrative and physical protections that are generally tied to a law, regulation, industry framework or contractual obligation;
(3) Standards provide organization-specific, quantifiable requirements for cybersecurity and data protection;
(4) Procedures (also known as Control Activities) establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives; and
(5) Guidelines are additional guidance that is recommended, but not mandatory.