



SECURE  
CONTROLS  
FRAMEWORK

# SECURE CONTROLS FRAMEWORK OVERVIEW & INSTRUCTIONS

version 2022.1

**con·trol**  
**/kən trol/**

**A control is the power to influence or direct behaviors and the course of events.** That is precisely why the Secure Controls Framework™ (SCF) was developed – we want to influence secure practices within organizations so that both cybersecurity and privacy principles are designed, implemented and managed in an efficient and sustainable manner.

*NOTE - This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity, privacy or audit professional to validate any compliance-related assumptions. For more information, please visit [www.SecureControlsFramework.com](http://www.SecureControlsFramework.com)*

## Table of Contents

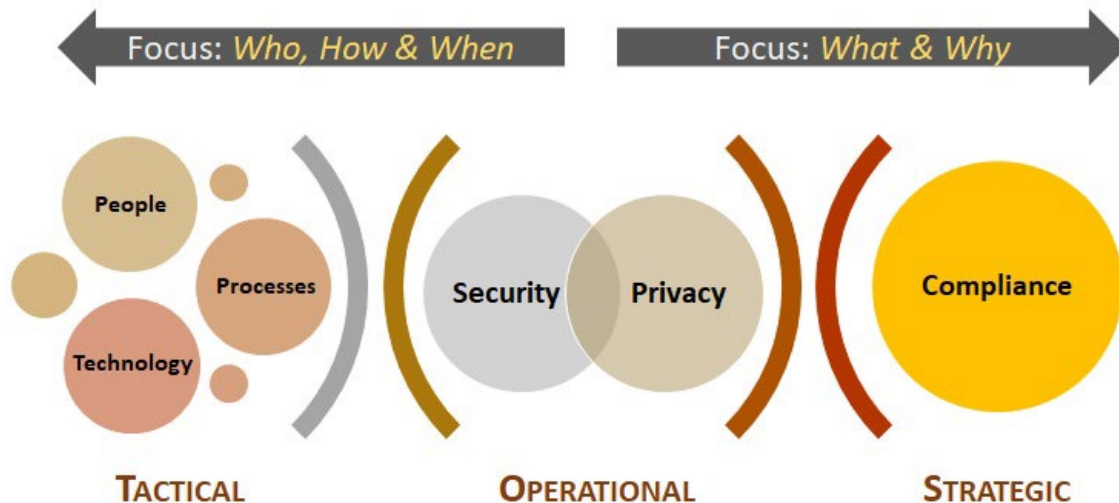
<b>Executive Summary .....</b>	<b>4</b>
<b>Level Setting What The SCF Is and It Is Not .....</b>	<b>5</b>
Why Should I Use The SCF? .....	5
What The SCF Is .....	5
What The SCF Is Not.....	5
Designing & Building An Audit-Ready Cybersecurity & Privacy Program .....	6
<b>Understanding What It Means To Adopt “Secure by Design” Principles .....</b>	<b>7</b>
Secure Practices Are Common Expectations .....	7
Compliance Should Be A Natural Byproduct of Secure Practices .....	7
Security & Privacy by Design (S P) Principles .....	8
SCF Privacy Management Principles .....	11
<b>Integrated Controls Management Approach To Using The SCF .....</b>	<b>13</b>
Applying ICM To Governance, Risk Management & Compliance (GRC) Functions.....	13
GRC Is A Plan, Do, Check & Act (PDCA) Adventure – That Is A Concept that Should Be Embraced, Not Fought Against.....	13
ICM Focuses On What It Means To Be “Secure & Compliant” .....	14
ICM Principles .....	14
<i>Principle 1: Establish Context</i> .....	14
<i>Principle 2: Define Applicable Controls</i> .....	14
<i>Principle 3: Assign Maturity-Based Criteria</i> .....	15
<i>Principle 4: Publish Policies &amp; Standards</i> .....	15
<i>Principle 5: Assign Stakeholder Accountability</i> .....	15
<i>Principle 6: Maintain Situational Awareness</i> .....	15
<i>Principle 7: Manage Risk</i> .....	15
<i>Principle 8: Evolve Processes</i> .....	15
<b>Practical Approach To Use The SCT To Implement ICM.....</b>	<b>16</b>
Establish Context .....	16
Define Applicable Controls .....	16
Assign Maturity-Based Criteria .....	17
Publish Policies & Standards .....	17
Assign Stakeholder Accountability.....	17
Maintain Situational Awareness .....	18
Manage Risk.....	18
Evolve Processes .....	18
<b>Security &amp; Privacy Capability Maturity Model (SP-CMM) .....</b>	<b>20</b>
SP-CMM: Defining What Right Looks Like .....	20
CCM vs Organization Size Considerations.....	21
<i>CMM 0 – Not Performed</i> .....	22
<i>CMM 1 – Performed Informally</i> .....	22
<i>CMM 2 – Planned &amp; Tracked</i> .....	22
<i>CMM 3 – Well-Defined</i> .....	22
<i>CMM 4 – Quantitatively Controlled</i> .....	23
<i>CMM 5 – Continuously Improving</i> .....	23
Defining A Capability Maturity “Sweet Spot” .....	24
<i>Negligence Considerations</i> .....	24
<i>Risk Considerations</i> .....	24
<i>Process Review Lag Considerations</i> .....	24
<i>Stakeholder Value Considerations</i> .....	24
SP-CMM Use Case #1 – Objective Criteria To Build A Cybersecurity & Privacy Program .....	25
<i>Identifying The Problem</i> .....	25

<i>Considerations</i> .....	25
SP-CMM Use Case #2 – Assist Project Teams To Appropriately Plan & Budget Secure Practices .....	26
<i>Identifying The Problem</i> .....	26
<i>Considerations</i> .....	26
SP-CMM Use Case #3 – Provide Objective Criteria To Evaluate Third-Party Service Provider Security .....	27
<i>Identifying The Problem</i> .....	27
<i>Considerations</i> .....	27
<b>Security &amp; Privacy Risk Management Model (SP-RMM) .....</b>	<b>28</b>
SP-RMM: Steps To Identify, Assess, Report & Mitigate Risk .....	29
1. <i>Identify Risk Management Principles</i> .....	29
2. <i>Identify, Implement &amp; Document Critical Dependencies</i> .....	29
3. <i>Formalize Risk Management Practices</i> .....	30
4. <i>Establish A Risk Catalog</i> .....	30
5. <i>Establish A Threat Catalog</i> .....	31
6. <i>Establish A Controls Catalog</i> .....	34
7. <i>Define Capability Maturity Model (CMM) Targets</i> .....	34
8. <i>Perform Risk Assessments</i> .....	35
9. <i>Establish The Context For Assessing Risks</i> .....	35
10. <i>Controls Gap Assessment</i> .....	35
11. <i>Assess Risks</i> .....	36
12. <i>Determine Risk</i> .....	36
13. <i>Prioritize &amp; Document Risks</i> .....	37
14. <i>Identify The Appropriate Management Audience</i> .....	37
15. <i>Management Determines Risk Treatment</i> .....	37
16. <i>Implement &amp; Document Risk Treatment</i> .....	37
<b>Pre-Defined Control Sets .....</b>	<b>38</b>
Business Mergers & Acquisitions (SCF-B) .....	38
Embedded Technology Controls (SCF-E) .....	38
US Government Contractor Controls (SCF-G) .....	38
Healthcare Controls (SCF-H) .....	38
Continuous Monitoring Controls (SCF-M) .....	38
Privacy Controls (SCF-P) .....	38
Ransomware Protection Controls (SCF-R) .....	38
Third-Party Risk Management Controls (SCF-T) .....	39

## EXECUTIVE SUMMARY

The Secure Controls Framework™ (SCF) focuses on internal controls. These are the cybersecurity and privacy-related policies, standards, procedures, technologies and associated processes that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected. The concept is to address the broader People, Processes, Technology and Data (PPTD) that are what controls fundamentally exists to govern.

Using the SCF should be viewed as a long-term tool to not only help with compliance-related efforts but to ensure security and privacy principles are properly designed, implemented and maintained. The SCF helps implement a holistic approach to protecting the Confidentiality, Integrity, Availability and Safety (CIAS) of your data, systems, applications and other processes. The SCF can be used to assist with strategic planning down to tactical needs that impact the people, processes and technologies directly impacting your organization.



This “best practices” guide covers the following topics:

- Level setting what the SCF is and what it is not;
- Integrated Controls Management (ICM) approach to Governance, Risk Management & Compliance (GRC);
- Leveraging the Security & Privacy Capability Maturity Model (SP-CMM);
- Leveraging the Security & Privacy Risk Management Model (SP-RMM); and
- Recommendations to tailor the control set for your needs to operationalize the SCF.

This document is designed for cybersecurity & privacy practitioners to gain an understanding of how the SCF is intended to be used in their organization.

## LEVEL SETTING WHAT THE SCF IS AND IT IS NOT

It is important for users of the SCF to understand what the SCF is and what it is not. We are very transparent on what the SCF offers and we want to help ensure that SCF users understand their role in using the SCF in their efforts to secure their organization.

### WHY SHOULD I USE THE SCF?

There is no sales pitch for using the SCF – it is a free resource so there is no financial incentive for us to make companies use it. For companies that have just one 1-2 compliance requirements, the SCF might be considered overkill for your needs. However, for companies that have 3+ compliance requirements (e.g., organization that has requirements to address ISO 27002, SOC 2, PCI DSS and GDPR), then the SCF is a great tool to streamline the management of cybersecurity and privacy controls.

In developing the SCF, we identified and analyzed over 100 statutory, regulatory and contractual frameworks. Through analyzing these thousands of legal, regulatory and framework requirements, we identified commonalities and this allows several thousand unique controls to be addressed by the over 1,000 controls that makeup the SCF. For instance, a requirement to maintain strong passwords is not unique, since it is required by dozens of laws, regulations and frameworks. This allows one well-worded SCF control to address multiple requirements. This focus on simplicity and sustainability is key to the SCF, since it can enable various teams to speak the same controls language, even though they may have entirely different statutory, regulatory or contractual obligations that they are working towards.



The SCF targets silos, since siloed practices within any organization are inefficient and can lead to poor security, due to poor communications and incorrect assumptions.

### WHAT THE SCF IS

The SCF is a comprehensive catalog of controls that is designed to enable companies to design, build and maintain secure processes, systems and applications. The SCF addresses both cybersecurity and privacy, so that these principles are designed to be “baked in” at the strategic, operational and tactical levels.

#### The SCF is:

- A control set.
- A useful tool to provide a “Rosetta Stone” approach to organizing cybersecurity and privacy controls so that the same controls can be used among companies and teams (e.g., privacy, cybersecurity, IT, project, procurement, etc.).
- Free for businesses to use. A result of a volunteer-led effort that uses “expert derived assessments” to perform the mapping from the controls to applicable laws, regulations and other frameworks.

The SCF also contains helpful guidance on possible tools and solutions to address controls. Additionally, it contains maturity criteria that can help an organization plan for and evaluate controls, based on a target maturity level.

### WHAT THE SCF IS NOT

While the SCF is a comprehensive catalog of controls that is designed to enable companies to design, build and maintain secure processes, systems and applications, the SCF will only ever be a control set and is not a “magic bullet” technology solution to address every possible cybersecurity and privacy compliance obligation that an organization faces.

#### The SCF is not:

- A substitute for performing due diligence and due care steps to understand your specific compliance needs.
- A complete technology or documentation solution to address all your security & privacy needs (e.g., the policies, standards, procedures and processes you need to have in place to be secure and compliant).
- Infallible or guaranteed to meet every compliance requirement your organization offers, since the controls are mapped based on expert-derived assessments to provide the control crosswalking that relies on human expertise and that is not infallible.

## DESIGNING & BUILDING AN AUDIT-READY CYBERSECURITY & PRIVACY PROGRAM

Building an audit-ready cybersecurity & privacy program requires addressing the holistic nature of security and privacy concerning how people, processes, technology and data impact existing security and data protection practices.

Building a security program that routinely incorporates security and privacy practices into daily operations requires a mastery of the basics. A useful analogy is with the children's toy, LEGO®. With LEGO® you can build nearly anything you want — either through following directions or using your own creativity. However, it first requires an understanding of how various LEGO® shapes either snap together or are incompatible.



Once you master the fundamentals with LEGO®, it is easy to keep building and become immensely creative since you know how everything interacts. However, when the fundamentals are ignored, the LEGO® structure will be weak and include systemic flaws. Security and privacy really are not much different, since those disciplines are made up of numerous building blocks that all come together to build secure systems and processes. The lack of critical building blocks will lead to insecure and poorly architected solutions.

When you envision each component that makes up a security or privacy “best practice” is a LEGO® block, it is possible to conceptualize how certain requirements are the foundation that form the basis for others components to attach to. Only when the all the building blocks come together and take shape do you get a functional security / privacy program!

Think of the SCF as a toolkit for you to build out your overall security program domain-by-domain so that cybersecurity and privacy principles are designed, implemented and managed by default!

## UNDERSTANDING WHAT IT MEANS TO ADOPT “SECURE BY DESIGN” PRINCIPLES

For an organization that just “does ISO”, it is easy to say, “We’re an ‘ISO shop’ and we exclusively use ISO 27001 cybersecurity principles for an Information Security Management System (ISMS)” and that would be routinely accepted as being adequate as a reasonable path to follow for many organizations. However, what about companies that have complex cybersecurity and compliance needs, such as a company that has to address SOC2, NIST SP 800-171, ISO 27002, CCPA, EU GDPR, PCI DSS, NY DFS, etc.? In these complex cases that involve multiple frameworks, ISO 27002 controls alone do not cut it. This is why it is important to understand what secure principles your organization is aligned with, so that the controls it implements are appropriate to build secure and compliant processes. What works for one company or industry does not necessarily work for another, since requirements are unique to the organization.

Most companies have requirements to document security and privacy processes, but lack the knowledge and experience to undertake such documentation efforts. That means organizations are faced to either outsource the work to expensive consultants or they ignore the requirement and hope they do not get in trouble for being non-compliant. In either situation, it is not a good place to be.

### SECURE PRACTICES ARE COMMON EXPECTATIONS

While the European Union General Data Protection Regulation (**EU GDPR**) made headlines by requiring organizations to demonstrate security & privacy principles are by both “by default and by design.” However, security & privacy engineering principles are not just limited to EU GDPR and are actually very common requirements, as shown below:

- NIST 800-53 - **SA-8**
- NIST Cybersecurity Framework - **PR.IP-2**
- ISO 27002 - **14.2.5 & 18.1.4**
- Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7012 (NIST 800-171) - **3.13.1 & 3.13.2**
- Federal Acquisition Regulations (FAR) **52.204-21 - 4**
- National Industrial Security Program Operating Manual (NISPOM) - **8-302 & 8-311**
- ISACA Trust Services Criteria (TSC) (SOC 2) - **CC3.2**
- Generally Accepted Privacy Principles (GAPP) - **4.2.3, 6.2.2, 7.2.2 & 7.2.3**
- New York State Department of Financial Service (DFS) - **23 NYCRR 500.08**
- Payment Card Industry Data Protection Standard (PCI DSS) - **2.2**
- Center for Internet Security Critical Security Controls (CIS CSC) - **1.2, 5.9, 6.2, 6.3, 6.4, 6.5, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.6, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 11.4, 11.5, 11.6, 11.7, 13.4, 13.5 & 16.5**



**SECURITY BY DESIGN (SbD)**



**PRIVACY BY DESIGN (PbD)**

### COMPLIANCE SHOULD BE A NATURAL BYPRODUCT OF SECURE PRACTICES

It is vitally important for any SCF user to understand that compliant does not mean secure. However, if you design, build and maintain secure systems, applications and processes, then compliance should be a natural byproduct of those secure practices.

The SCF’s comprehensive listing of over 1,000 cybersecurity and privacy controls is categorized into 32 domains that are mapped to over 100 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the security & privacy principles to help an organization ensure that secure practices are implemented by design and by default.



You may be asking yourself, “*What security & privacy principles should I be using?*” and that is a great question. The SCF helped with this common question by taking the 32 domains of the SCF and creating principles that an organization can use. The idea is that by focusing on these secure principles, an organization will design, implement and maintain secure systems, applications and processes that will by default help the organization comply with its compliance obligations.

## SECURITY & PRIVACY BY DESIGN (S|P) PRINCIPLES

The concept of building security and privacy into technology solutions both by default and by design is a basic expectation for businesses, regardless of the industry. The adoption of security and privacy principles is a crucial step in building a secure, audit-ready program.

The S|P is a set of 32 security and privacy principles that leverage the SCF's extensive cybersecurity and privacy control set. You can download the free poster by [clicking the image to the right](#).



The “S pipe P” logo is a nod to the computing definition of the | or “pipe” symbol (e.g., shift + backslash), which is a computer command line mechanism that allows the output of one process to be used as input to another process. In this way, a series of commands can be linked to more quickly and easily perform complex, multi-stage processing. Essentially, the concept is that security principles are being “piped” with privacy principles to create secure processes in an efficient manner.

The S|P establishes 32 common-sense principles to guide the development and oversight of a modern security and privacy program. Those 32 S|P principles are listed below:

#	SCF Domain	Identifier	Security & Privacy by Design (S P) Principle	S P Principle Intent
1	Security & Privacy Governance	GOV	Govern a documented, risk-based program that encompasses appropriate security and privacy principles to address all applicable statutory, regulatory and contractual obligations.	Organizations specify the development of an organization’s security and privacy programs, including criteria to measure success, to ensure ongoing leadership engagement and risk management.
2	Asset Management	AST	Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset’s location.	Organizations ensure technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal, ensuring only authorized devices are allowed to access the organization’s network and to protect the organization’s data that is stored, processed or transmitted on its assets.
3	Business Continuity & Disaster Recovery	BCD	Maintain the capability to sustain business-critical functions while successfully responding to and recovering from incidents through a well-documented and exercised process.	Organizations establish processes that will help the organization recover from adverse situations with the minimal impact to operations, as well as provide the ability for e-discovery.
4	Capacity & Performance Planning	CAP	Govern the current and future capacities and performance of technology assets.	Organizations prevent avoidable business interruptions caused by capacity and performance limitations by proactively planning for growth and forecasting, as well as requiring both technology and business leadership to maintain situational awareness of current and future performance.
5	Change Management	CHG	Govern change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.	Organizations ensure both technology and business leadership proactively manage change. This includes the assessment, authorization and monitoring of technical changes across the enterprise so as to not impact production systems uptime, as well as allow easier troubleshooting of issues.



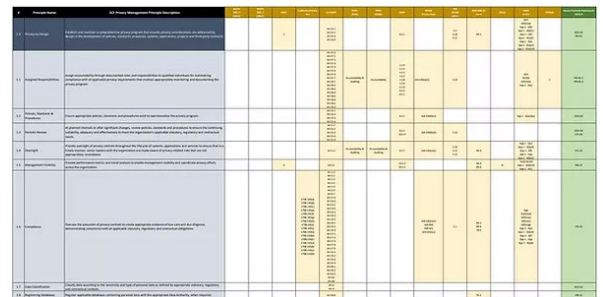
6	Cloud Security	CLD	Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal controls.	Organizations govern the use of private and public cloud environments (e.g., IaaS, PaaS and SaaS) to holistically manage risks associated with third-party involvement and architectural decisions, as well as to ensure the portability of data to change cloud providers, if needed.
7	Compliance	CPL	Oversee the execution of cybersecurity and privacy controls to create appropriate evidence of due care and due diligence, demonstrating compliance with all applicable statutory, regulatory and contractual obligations.	Organizations ensure controls are in place to be aware of and comply with applicable statutory, regulatory and contractual compliance obligations, as well as internal company standards.
8	Configuration Management	CFG	Govern the establishment and ongoing management of secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.	Organizations establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features can be inadvertently or deliberately omitted or rendered inoperable, allowing processing irregularities to occur or the execution of malicious code.
9	Continuous Monitoring	MON	Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.	Organizations establish and maintain ongoing situational awareness across the enterprise through the centralized collection and review of security-related event logs. Without comprehensive visibility into infrastructure, operating system, database, application and other logs, the organization will have "blind spots" in its situational awareness that could lead to system compromise, data exfiltration, or unavailability of needed computing resources.
10	Cryptographic Protections	CRY	Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive data both at rest and in transit.	Organizations ensure the confidentiality of the organization's data through implementing appropriate cryptographic technologies to protect systems and data.
11	Data Classification & Handling	DCH	Publish and enforce a data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.	Organizations ensure that technology assets, both hardware and media, are properly classified and measures implemented to protect the organization's data from unauthorized disclosure, regardless if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance requirements dictate the minimum safeguards that must be in place to protect the confidentiality, integrity and availability of data.
12	Embedded Technology	EMB	Provide additional scrutiny to the risks associated with embedded technology, based on the potential damages posed when used maliciously.	Organizations specify the development, proactive management and ongoing review of security embedded technologies, including hardening of the "stack" from the hardware, to firmware, software, transmission and service protocols used for Internet of Things (IoT) and Operational Technology (OT) devices.
13	Endpoint Security	END	Harden endpoint devices to protect against reasonable threats to those devices and the data they store, transmit and process.	Organizations ensure that endpoint devices are appropriately protected from security threats to the device and its data. Applicable statutory, regulatory and contractual compliance requirements dictate the minimum safeguards that must be in place to protect the confidentiality, integrity, availability and safety considerations.
14	Human Resources Security	HRS	Foster a security and privacy-minded workforce through sound hiring practices and ongoing personnel management.	Organizations create a security and privacy-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward and collaboration.

15	Identification & Authentication	IAC	Implement an Identity and Access Management (IAM) capability to ensure the concept of “least privilege” is consistently implemented across all systems, applications and services for individual, group and service accounts.	Organizations implement the concept of “least privilege” through limiting access to the organization’s systems and data to authorized users only.
16	Incident Response	IRO	Maintain a practiced incident response capability that trains all users on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with an Incident Response Plan (IRP).	Organizations establish and maintain a capability to guide the organization’s response when security or privacy-related incidents occur and to train users how to detect and report potential incidents.
17	Information Assurance	IAO	Utilize an impartial assessment process to validate the existence and functionality of appropriate security and privacy controls, prior to a system, application or service being used in a production environment.	Organizations ensure the adequacy of security and controls are appropriate in both development and production environments.
18	Maintenance	MNT	Utilize secure practices to maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.	Organizations ensure that technology assets are properly maintained to ensure continued performance and effectiveness. Maintenance processes apply additional scrutiny to the security of end-of-life or unsupported assets.
19	Mobile Device Management	MDM	Govern mobile devices through a centralized or decentralized model to restrict logical and physical access to the devices, as well as the amount and type of data that can be stored, transmitted or processed.	Organizations govern risks associated with mobile devices, regardless if the device is owned by the organization, its users or trusted third-parties. Wherever possible, technologies are employed to centrally manage mobile device access and data storage practices.
20	Network Security	NET	Architect a defense-in-depth methodology that enforces the concept of “least functionality” through restricting network access to systems, applications and services.	Organizations ensure sufficient security and privacy controls are architected to protect the confidentiality, integrity, availability and safety of the organization’s network infrastructure, as well as to provide situational awareness of activity on the organization’s networks.
21	Physical & Environmental Security	PES	Implement layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.	Organizations minimize physical access to the organization’s systems and data by addressing applicable physical security controls and ensuring that appropriate environmental controls are in place and continuously monitored to ensure equipment does not fail due to environmental threats.
22	Privacy	PRI	Implement a privacy program that ensures industry-recognized privacy practices are identified and operationalized throughout the lifecycle of systems, applications and services.	Organizations align privacy engineering decisions with the organization’s overall privacy strategy and industry-recognized leading practices to secure Personal Information (PI) that implements the concept of privacy by design and by default.
23	Project & Resource Management	PRM	Utilize a risk-based approach to prioritize the planning and resourcing of all security and privacy aspects for projects and other initiatives to alleviate foreseeable governance, risk and compliance roadblocks.	Organizations ensure that security-related projects have both resource and project/program management support to ensure successful project execution.
24	Risk Management	RSK	Govern a risk management capability that ensures risks are consistently identified, assessed, categorized and appropriately remediated.	Organizations ensure that security and privacy-related risks are visible to and understood by the business unit(s) that own the assets and / or processes involved. The security and privacy teams only advise and educate on risk management matters, while it is the business units and other key stakeholders who ultimately own the risk.

25	Secure Engineering & Architecture	SEA	Implement secure engineering and architecture processes to ensure industry-recognized secure practices are identified and operationalized throughout the lifecycle of systems, applications and services.	Organizations align cybersecurity engineering and architecture decisions with the organization's overall technology architectural strategy and industry-recognized leading practices to secure networked environments.
26	Security Operations	OPS	Assign appropriately-qualified personnel to deliver security and privacy operations that provide reasonable protective, detective and responsive services.	Organizations ensure appropriate resources and a management structure exists to enable the service delivery of cybersecurity operations.
27	Security Awareness & Training	SAT	Develop a security and privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.	Organizations develop a security and privacy-minded workforce through continuous education activities and practical exercises, in order to refine and improve on existing training.
28	Technology Development & Acquisition	TDA	Govern the development process for any acquired or developed system, application or service to ensure secure engineering principles are operationalized and functional.	Organizations ensure that security and privacy principles are implemented into any products/solutions that are either developed internally or acquired to make sure that the concepts of "least privilege" and "least functionality" are incorporated.
29	Third-Party Management	TPM	Implement ongoing third-party risk management practices to actively oversee the supply chain so that only trustworthy third-parties are used.	Organizations ensure that security and privacy risks associated with third-parties are minimized and enable measures to sustain operations should a third-party become defunct.
30	Threat Management	THR	Identify, assess and remediate technology-related threats to assets and business processes, based on a thorough risk analysis to determine the potential risk posed from the threat.	Organizations establish a capability to proactively identify and manage technology-related threats to the security and privacy of the organization's systems, data and business processes.
31	Vulnerability & Patch Management	VPM	Utilize a risk-based approach to vulnerability and patch management practices that minimizes the attack surface of systems, applications and services.	Organizations proactively manage the risks associated with technical vulnerability management that includes ensuring good patch and change management practices are utilized.
32	Web Security	WEB	Govern all Internet-facing technologies to ensure those systems, applications and services are securely configured and monitored for anomalous activity.	Organizations address the risks associated with Internet-accessible technologies by hardening devices, monitoring system file integrity, enabling auditing, and monitoring for malicious activities.

## SCF PRIVACY MANAGEMENT PRINCIPLES

Through our interactions with organizations, we identified that many organizations understand the cybersecurity framework they wanted or needed to align with, but had no understanding of the privacy principles their organization should be aligned with. We set out to fix that issue and what we did was select over a dozen of the most common privacy frameworks to create a "best in class" approach to managing privacy principles. The best part is these are all mapped to the SCF and is built into the SCF, so you can leverage the SCF for both your cybersecurity and privacy needs!



Why should you care? When you tie the broader S|P in with the SCF Privacy Management Principles, you have an excellent foundation for building and maintaining secure systems, applications and services that address cybersecurity and privacy considerations by default and by design.

Think of the SCF Privacy Management Principles as a supplement to the S|P to assist in defining and managing privacy principles, based on selected privacy frameworks. This can enable your organization to align with multiple privacy frameworks that also map to your cybersecurity and privacy control set, since we found the "apples to oranges" comparison between disparate privacy frameworks was difficult for most non-privacy practitioners to comprehend.

Below are the seventeen (17) different frameworks the SCF Privacy Management Principles is mapped to:

- AICPA's Trust Services Criteria (**TSC**) SOC 2
- Asia-Pacific Economic Cooperation (**APEC**)
- California Consumer Privacy Act (**CCPA**)
- European Union General Data Protection Regulation (**EU GDPR**)
- Fair Information Practice Principles (**FIPPs**) - Department of Homeland Security (**DHS**) / Office of Management and Budget (**OMB**)
- Generally Accepted Privacy Principles (**GAPP**)
- HIPAA Privacy Rule
- ISO 27701
- ISO 29100
- Nevada SB820
- NIST SP 800-53 R4
- NIST SP 800-53 R5
- NIST Privacy Framework v1.0
- Organization for Economic Co-operation and Development (**OECD**)
- Office of Management and Budget (**OMB**) - Circular A-130
- Personal Information Protection and Electronic Documents Act (**PIPEDA**)

The seventy-nine (79) principles of the SCF Privacy Management Principle are organized into eleven (11) domains:

1. Privacy by Design
2. Data Subject Participation
3. Limited Collection & Use
4. Transparency
5. Data Lifecycle Management
6. Data Subject Rights
7. Security by Design
8. Incident Response
9. Risk Management
10. Third-Party Management
11. Business Environment

## INTEGRATED CONTROLS MANAGEMENT APPROACH TO USING THE SCF

The Integrated Controls Management (ICM) is a joint project between the SCF and [ComplianceForge](#). The premise of the ICM is that controls are central to cybersecurity and privacy operations, as well as the overall business rhythm of an organization. This is supported by the [Security & Privacy Risk Management Model \(SP-RMM\)](#), that describes the centralized nature of controls, where not just policies and standards map to controls, but procedures, metrics, threats and risks, as well.

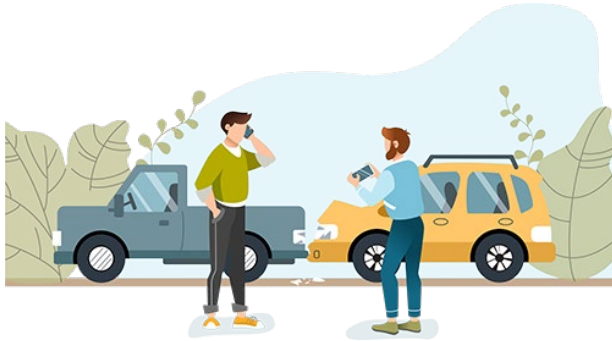
ICM is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization's cybersecurity and privacy operations. ICM is designed to proactively address the strategic, operational and tactical nature of operating an organization's cybersecurity and privacy program at the control level. ICM is designed to address both internal controls, as well as the broader concept of Supply Chain Risk Management (SCRM).

### APPLYING ICM TO GOVERNANCE, RISK MANAGEMENT & COMPLIANCE (GRC) FUNCTIONS

GRC can be a costly and labor-intensive endeavor, so what justifies the investment? Essentially, GRC functions help avoid negligence, with the added benefit of improved IT/cyber/privacy operating effectiveness. The reality of the situation is your company invests in cybersecurity and privacy as a necessity. This necessity is driven in large part by laws, regulations and contractual requirements that it is legally obligated to comply with. It is also driven by the desire to protect its public image from damaging acts that happen when cybersecurity and privacy practices are ignored. Regardless of the specific reason, those charged with developing, implementing and running your organization's cybersecurity and data protection program must do so in a reasonable manner that would withstand scrutiny that could take the form of an external auditor, regulator or prosecuting attorney.

**How fast would you drive your car if you didn't have any brakes?** Think about that for a moment - you would likely drive at a crawl in first gear and even then you would invariably have accidents as you bump into objects and other vehicles to slow down. Brakes on a vehicle actually allow you to drive fast, in addition to safely navigating dangers on the road!

While it is not the most flattering analogy, GRC is akin to the brakes on your car, where they enable a business' operations to go fast and avoid catastrophic accidents. Without those "brakes", an accident is a certainty! These brakes that enable a business' operations to stay within the guardrails are its cybersecurity policies, standards and procedures. These requirements constitute "reasonable practices" that the organization is required to implement and maintain to avoid being negligent.



### GRC IS A PLAN, DO, CHECK & ACT (PDCA) ADVENTURE – THAT IS A CONCEPT THAT SHOULD BE EMBRACED, NOT FOUGHT AGAINST

GRC most often deals with legally-binding requirements, so it is important to understand that negligence is situationally-dependent. For example, an intoxicated driver who gets behind the wheel acting negligently. However, when sober, that same individual is a champion race car driver who is highly skilled and would not be considered incompetent in any regard. In this example, driving intoxicated constitutes a negligent act and shows that negligence has nothing to do with being incompetent. The point is to demonstrate that an organization can employ many highly-competent personnel, but even competent people can behave in a negligent manner. GRC fundamentally exists to help an organization avoid circumstances that could be construed as negligent acts.

Considering how business practices continuously evolve, so must cybersecurity practices. The PDCA process (also referred to as the Deming Cycle) enables the GRC function to continuously evaluate risks, threats and performance trends, so that the organization's leadership can take the necessary steps to minimize risk by modifying how people, processes and technology work together to keep everything both secure and operational. The PDCA approach is a logical way to conceptualize how GRC works:

- **Plan.** The overall process begins with planning. At its core, this phase is the process of conducting due diligence. The results of this process will define necessary controls (e.g., requirements) that influence the need for policies, standards and procedures. These actions directly influence resourcing and procurement actions that range from staffing needs to tool purchases and services acquisition.
- **Do.** This phase is the process of conducting due care, where it is focused on the "reasonable care" necessary to properly and sufficiently conduct operations that demonstrate the absence of negligence. This is the execution of procedures – the processes that bring controls to life.
- **Check** This phase can be considered maintaining situational awareness. There are several ways to maintain situation awareness and that ranges from control validation testing to audits/assessments and metrics.

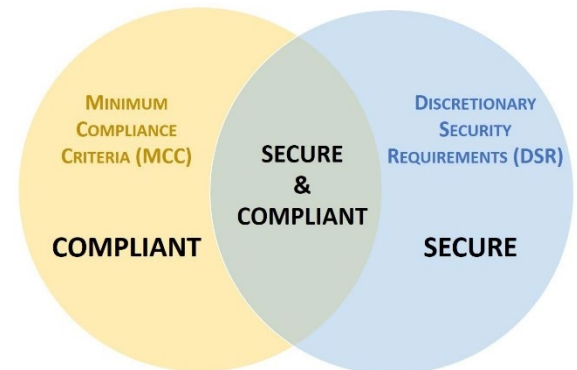


- **Act**- This phase again brings up the concept of “reasonable care” that necessitates taking action to maintain the organization’s targeted risk tolerance threshold. This deals with addressing two main concepts (1) real deficiencies that currently exist and (2) areas of concern that may expose the organization to a threat if no action is taken.

## ICM FOCUSES ON WHAT IT MEANS TO BE “SECURE & COMPLIANT”

ICM specifically focuses on the need to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions. To assist in this process, ICM helps an organization categorize its applicable controls according to “must have” vs “nice to have” requirements:

- 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:

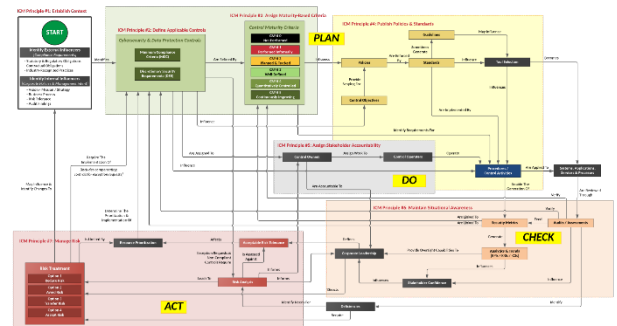
- MCC are primarily externally-influenced, based on industry, government, state and local regulations. MCC should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization’s respective 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 premise is that controls are central to cybersecurity and privacy operations as well as the business rhythms of the organization. Without properly defining MCC and DSR thresholds, an organization’s overall cybersecurity and privacy program is placed in jeopardy as the baseline practices are not anchored to clear requirements. Furthermore, understanding and clarifying the difference between "compliant" versus "secure" (e.g., MCC vs. MCC+DSR) enhances risk management discussions.

## ICM PRINCIPLES

There are eight (8) principles associated with ICM:

1. Establish Context
2. Define Applicable Controls
3. Assign Maturity-Based Criteria
4. Publish Policies, Standards & Procedures
5. Assign Stakeholder Accountability
6. Maintain Situational Awareness
7. Manage Risk
8. Evolve Processes



[graphic can be downloaded from <https://graphics.complianceforge.com/icm/ICM-PCDA.pdf>]

### PRINCIPLE 1: ESTABLISH CONTEXT

To build and maintain efficient and effective operations, a cybersecurity & privacy program must have a hierarchical vision, mission and strategy that directly supports the organization’s broader strategic objectives and business processes. This process of establishing context involves identifying all applicable external compliance requirements (e.g., laws, regulations and contractual obligations), as well as internal directives (e.g., Board of Directors, corporate policies, etc.). This is a due diligence element of the cybersecurity and privacy program.

### PRINCIPLE 2: DEFINE APPLICABLE CONTROLS

A tailored control set cybersecurity and data protection controls must exist. This control set needs to be made of Minimum Compliance Criteria (MCC) and Discretionary Security Requirements (DSR). This blend of “must have” and “nice to have” requirements establish an organization’s tailored control set to ensure both secure practices and compliance.

**PRINCIPLE 3: ASSIGN MATURITY-BASED CRITERIA**

The cybersecurity & privacy program must assign maturity targets to define organization-specific “what right looks like” for controls. This establishes attainable criteria for people, processes and technology requirements. Tailored maturity level criteria can be used to plan for, budget for and assess against. Maturity targets should support the organization’s need for operational resiliency.

**PRINCIPLE 4: PUBLISH POLICIES & STANDARDS**

Documentation must exist, otherwise an organization’s cybersecurity and data protection practices are unenforceable. Formalizing organization-specific requirements via policies and standards are necessary to operationalize controls. Documented policies and standards provide evidence of due diligence that the organization identified and implemented reasonable steps to address its applicable requirements.

**PRINCIPLE 5: ASSIGN STAKEHOLDER ACCOUNTABILITY**

Controls must be assigned to stakeholders to ensure accountability (e.g., business units, teams and/or individuals). These “control owners” may assign the task of executing controls to “control operators” at the Individual Contributors (IC)-level. Stakeholders utilize the prescriptive requirements from policies and standards to develop Standardized Operating Procedures (SOP) that enable ICs to execute those controls. The documented execution of procedures provides evidence of due care that reasonable practices are being performed.

**PRINCIPLE 6: MAINTAIN SITUATIONAL AWARENESS**

Situational awareness must involve more than merely “monitoring controls” (e.g., metrics). While metrics are a point-in-time snapshot into discrete controls’ performance, the broader view of metrics leads to a longer-term trend analysis. When properly tied in with current risk, threat and vulnerability information, this insight provides “situational awareness” that is necessary for organizational leadership to adjust plans to operate within the organization’s risk threshold.

**PRINCIPLE 7: MANAGE RISK**

Proactive risk management processes must exist across all phases of development/information/system life cycles to address confidentiality, integrity, availability and safety aspects. Risk management must address internal and external factors, including privacy and Supply Chain Risk Management (SCRM) considerations. To manage risk, it requires the organization to enforce a clearly defined risk threshold and ensure reasonable security practices are operational.

**PRINCIPLE 8: EVOLVE PROCESSES**

Cybersecurity and data protection measures must adapt and evolve to address business operations and the evolving threat landscape. This requires the adoption of a Plan, Do, Check & Act (PDCA) approach (Deming Cycle) to ensure the organization proactively identifies its requirements, implements appropriate protections, maintains situational awareness to detect incidents, operates a viable capability to respond to incidents and can sustain key business operations, if an incident occurs.



## PRACTICAL APPROACH TO USE THE SCT TO IMPLEMENT ICM

ICM is meant to be put into practice by organizations of any size or industry. The information below provides an understanding of available options to implement ICM with existing solutions. The SCF is a great way to implement the ICM.

### ESTABLISH CONTEXT

Part of your due diligence process is to establish the context of the scope for cybersecurity and privacy controls. Practical steps to establish context includes:

- Read through the S|P principles to familiarize yourself with the 32 domains to understand how they come together to address the cybersecurity, privacy and physical security considerations for a modern security program.
- Talk with representatives outside of IT and cybersecurity to gain an appreciation of other compliance requirements (e.g., legal, procurement, physical security, etc.).
- Come up with a list of the “must have” laws, regulations and frameworks that your organization must comply with.
- Come up with a list of “nice to have” requirements that your Board of Directors, or other stakeholders, feel are necessary.

Understanding the requirements for both cybersecurity and privacy principles involves a simple process of distilling expectations. This process is all part of documenting reasonable expectations that are “right-sized” for an organization, since every organization has unique requirements.

Some people freak out and think they have to do all 1,000+ controls in the SCF and that is just not the case. It is best to visualize the SCF as a “buffet of cybersecurity and privacy controls,” where there is a selection of 1,000+ controls available to you. You as you do not eat everything possible on a buffet table, the same applies to the SCF’s control set. Once you know what is applicable to you, you can generate a customized control set that gives you just the controls you need to address your statutory, regulatory and contractual obligations.

The approach looks at the following spheres of influence to identify applicable SCF controls:

- Statutory obligations - These are laws (e.g., US state, federal and international laws).
- Regulatory obligations - These are requirements from regulatory bodies or governmental agencies.
- Contractual obligations - These are requirements that are stipulated in contracts, vendor agreements, etc.
- Industry-recognized practices - These are requirements that are based on an organization’s specific industry that are considered reasonably-expected practices.

Please keep in mind that the SCF is a tool and it is only as good as its used – just like a pocketknife shouldn’t be used as a prybar. Realistically, if you do not scope the controls from the SCF correctly, you will not address your applicable compliance requirements since you are missing what is expected. That is not a deficiency of the SCF – that is simply negligence on the part of the user of the tool.

To make sure scoping is done properly, it is imperative for you to speak with your legal, IT, project management, cybersecurity and procurement teams (and other stakeholders you may feel are relevant to scoping controls). The reason for this collaboration is so that you can get a complete picture of all the applicable laws, regulations and frameworks that your organization is legally obligated to comply with. Those teams will likely provide the best insights into what is required and that list of requirements then makes it simple to go through and customize the SCF for your specific needs!

### DEFINE APPLICABLE CONTROLS

There is a column that exists in the SCF to help with the task of defining applicable controls. It is a column called the “Minimum Security Requirements (**MSR**) Filter” that will assist you in this process.

The SCF is fundamentally an Excel spreadsheet. Therefore, you can use your Excel skills to manually filter the requirements. If you are comfortable in Excel, it might take you 5-10 minutes to do this filtering, based on how many requirements you need to map to.

As previously mentioned, the ICM is focused on defining “must have” vs “nice to have” requirements:

- 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.
- Minimum Security Requirements (**MSR**) is the resulting set of controls necessary to be “compliant and secure” to manage your organization’s cybersecurity and privacy program.

Follow these steps:

1. Either hide or delete all of the columns containing laws, regulations or frameworks that are not applicable to your organization (e.g., if you only have to comply with ISO 27002, PCI DSS and EU GDPR, then you can delete or hide all other mapping columns but those).
2. Using the filter option in Excel (little gray arrow on the top row in each column), you would then filter the columns to only show cells that contain content (e.g., don't show blank cells in that column).
3. In that **MCC column**, simply put an "x" to mark that control as being "must have" controls. In the **DSR column**, simply put an "x" to mark that control as being "nice to have" controls. A selection of either MCC or DSR will select MSR. Do this for all the rows shown in that column.
4. Unfilter the column you just performed this task on and do it to the next law, regulation or framework that you need to map.
5. Repeat step 3 and step 4 until all your applicable laws and regulations are mapped to.
6. The **MSR column** will now have an "x" that marks each SCF control that is applicable for your needs, based on what was selected for MCC and DSR controls.

FX	FY	FZ
Minimum Security Requirements MCC + DSR	Identify Minimum Compliance Controls (MCC)	Identify Discretionary Security Requirements (DSR)
x	x	
x		x

This will leave you with a SCF control set that is tailored for your specific needs.

### ASSIGN MATURITY-BASED CRITERIA

From the previous step, you identified the controls that are applicable to your specific needs (e.g., MCC + DSR). You can now use the SP-CMM criteria to "define what right looks like" for each control.

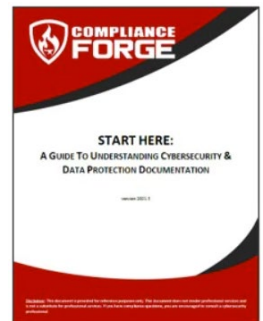
*Note: The SCF will not tell you what you should select, since that is a due diligence step that you have to address, based on the risk tolerance that your organization is willing to accept.*

### PUBLISH POLICIES & STANDARDS

There are generally three options to obtaining cybersecurity and privacy documentation:

1. Use internal resources to write it in-house;
2. Hire a consultant to write a bespoke set of documentation; or
3. Purchase semi-customized templates online.

ComplianceForge wrote a [document](#) to help organizations understand cybersecurity and privacy documentation. This guide is a free resource to educate organizations on what proper cybersecurity and data protection documentation, based on definitions from authoritative sources. These policies and standards provide the requirements that your organization has to adhere to.



### ASSIGN STAKEHOLDER ACCOUNTABILITY

Assigning stakeholder accountability offers unique challenges for organizations, since it is beyond IT, cybersecurity and privacy. Common stakeholders involves Human Resources (HR), procurement, facilities management, legal and many other teams to ensure accountability is enforceable. Realistically, this step is an executive-management function since it require inter-departmental enforcement by organizational management.

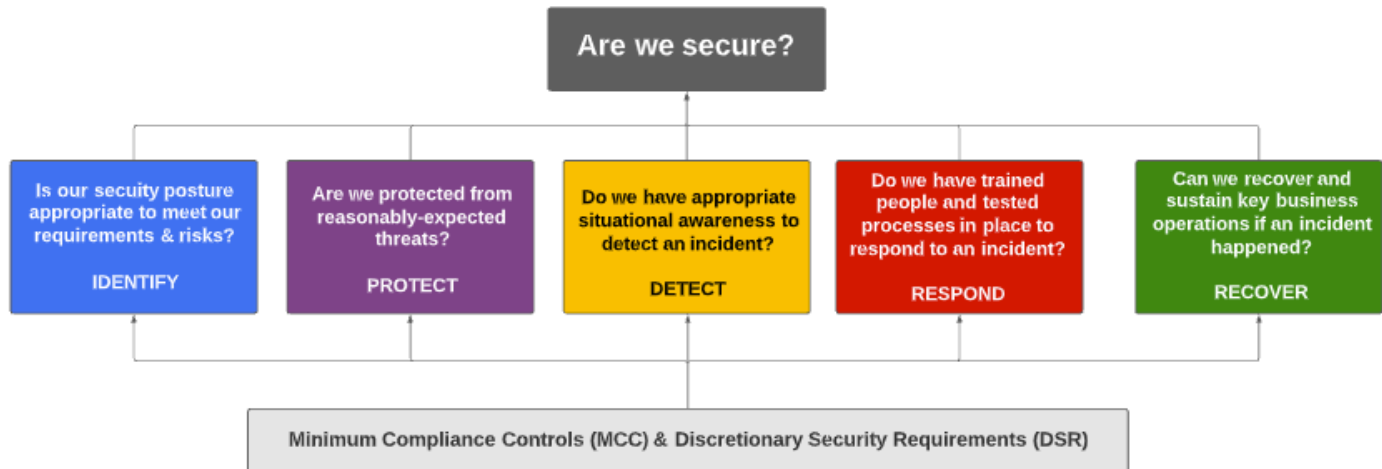
A great starting point is the NIST SP 800-181, *Workforce Framework for Cybersecurity (NICE Framework)*.<sup>1</sup> The NICE Framework offers an efficient way to assign stakeholder accountability for internal and external stakeholders.

<sup>1</sup> NIST SP 800-181 - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

## MAINTAIN SITUATIONAL AWARENESS

Maintaining situational awareness has different meanings, based on the security culture of an organization. For some organizations, it means metrics, while for others it means a broader understanding of control performance, risks, threats and current vulnerability information.

The ComplianceForge [Security Metrics Reporting Model™ \(SMRM\)](#) takes a practical view towards implementing a sustainable metrics reporting capability. At the end of the day, executive management (e.g., CIO, CEO, Board of Directors (BoD), etc.) often just want a simple answer to a relatively-straightforward question: “Are we secure?”



In order for a CISO to honestly provide an answer, it requires a way for the CISO to measure and quantify an “apples and oranges” landscape where processes and technologies lack both uniform risk weighting and abilities to capture metrics.

## MANAGE RISK

There are many ways to management risk. However, the SP-RMM contains a control-centric:

- Risk catalog;
- Threat catalog; and
- Methodology to perform a risk assessment.

The value of the SP-RMM is having a standardized methodology where controls are tied to specific risks and threats. Based on the other criteria offered by the SCF (e.g., weighting and maturity criteria), the SP-RMM makes calculating risk a straightforward process.

## EVOLVE PROCESSES

The ComplianceForge [Integrated Cybersecurity Governance Model™ \(ICGM\)](#) takes a comprehensive view towards governing a cybersecurity and privacy program. Without an overarching concept of operations for the broader GRC/IRM function, organizations will often find that their governance, risk management, compliance and privacy teams are siloed in how they think and operate. These siloed functions and unclear roles often stem from a lack of a strategic understanding of how these specific functions come together to build a symbiotic working relationship between the individual teams that enables quality control over people, processes and technology.

The ICGM utilizes a Plan, Do, Check & Act (**PDCA**) approach that is a logical way to design a governance structure:

- Plan. The overall ICM process begins with planning. This planning will define the policies, standards and controls for the organization. It will also directly influence the tools and services that an organization purchases, since technology purchases should address needs that are defined by policies and standards.
- Do. Arguably, this is the most important section for cybersecurity and privacy practitioners. Controls are the “security glue” that make processes, applications, systems and services secure. Procedures (also referred to as control activities) are the processes how the controls are actually implemented and performed.
- Check. In simple terms, this is situational awareness. Situational awareness is only achieved through reporting through metrics and reviewing the results of audits/assessments.
- Act. This is essentially risk management, which is an encompassing area that deals with addressing two main concepts (1) real deficiencies that currently exist and (2) possible threats to the organization.

19 of 39

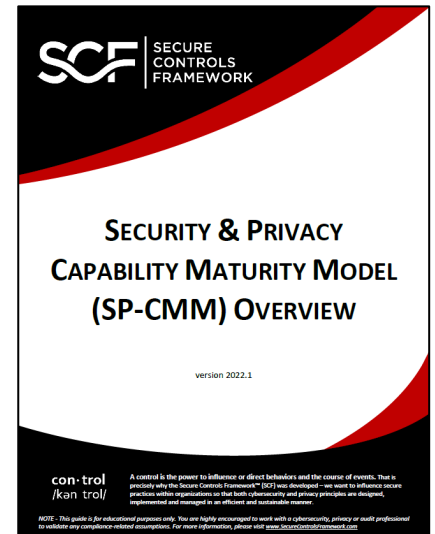
## SECURITY & PRIVACY CAPABILITY MATURITY MODEL (SP-CMM)

The SCF has built-in maturity criteria for each control. The SP-CMM is meant to solve the problem of objectivity in both establishing and evaluating cybersecurity and privacy controls.

There are three (3) main objectives for the SP-CMM:

1. Provide CISO/CPOs/CIOs with objective criteria that can be used to establish expectations for a cybersecurity & privacy program;
2. Provide objective criteria for project teams so that secure practices are appropriately planned and budgeted for; and
3. Provide minimum criteria that can be used to evaluate third-party service provider controls.

There are likely many other use cases that the SP-CMM can be used, but those three objectives listed above drove the development of this project. The reason for this simply comes down to a need by businesses, regardless of size or industry, for a solution that can help fix those three common frustrations that exist in most cybersecurity and privacy programs. We want to help eliminate, or at least minimize, the Fear, Uncertainty & Doubt (**FUD**) that is used to justify purchases and/or evaluate controls by injecting objectivity into the process.

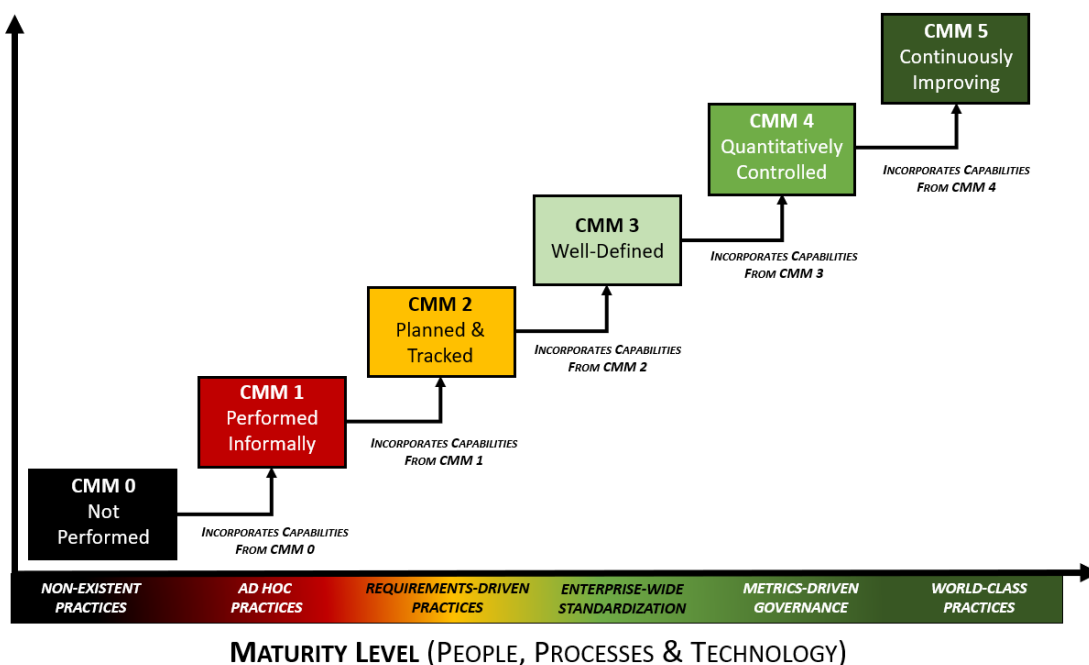


### SP-CMM: DEFINING WHAT RIGHT LOOKS LIKE

The SP-CMM draws upon the high-level structure of the Systems Security Engineering Capability Maturity Model v2.0 (**SSE-CMM**), since we felt it was the best model to demonstrate varying levels of maturity for people, processes and technology at a control level. If you are unfamiliar with the SSE-CMM, it is well-worth your time to read through the SSE-CMM Model Description Document that is hosted by the US Defense Technical Information Center (**DTIC**).<sup>2</sup>

The six (6) SP-CMM levels are:

- CMM 0 – Not Performed
- CMM 1 – Performed Informally
- CMM 2 – Planned & Tracked
- CMM 3 – Well-Defined
- CMM 4 – Quantitatively Controlled
- CMM 5 – Continuously Improving



<sup>2</sup> SSE-CMM - <https://apps.dtic.mil/dtic/tr/fulltext/u2/a393329.pdf>

## CCM VS ORGANIZATION SIZE CONSIDERATIONS

The following table summarizes the high-level expectations for small/medium/large organizations to meet each level of maturity.

Maturity Level	Small Organizations	Medium Organizations	Large Organizations
<b>SP-CMM 0</b>	<ul style="list-style-type: none"> <li>Lack of processes would be considered negligent behavior. This is generally due to a lack of a cybersecurity and privacy program.</li> <li><b>[NEGLIGENT]</b></li> </ul>		It is unlikely for a large organization to completely ignore cybersecurity and privacy requirements.
<b>SP-CMM 1</b>	<ul style="list-style-type: none"> <li>IT support focuses on reactionary “break / fix” activities and are ad hoc in nature.</li> <li>IT support is likely outsourced with a limited support contract.</li> <li><b>[LIKELY NEGLIGENT]</b></li> </ul>	<ul style="list-style-type: none"> <li>Internal IT staff exists, but there is no management support to spend time or budget on security / privacy controls that leads to ad hoc control implementation.</li> <li>Focus is on general IT operations without clear standards that implement secure systems and processes.</li> <li><b>[LIKELY NEGLIGENT]</b></li> </ul>	
<b>SP-CMM 2</b>	<ul style="list-style-type: none"> <li>Internal IT role(s) has clear requirements and is supported to meet applicable cybersecurity / privacy compliance obligations; or</li> <li>The outsourced IT provider is properly scoped in its support contract to address applicable compliance obligations.</li> </ul>	<ul style="list-style-type: none"> <li>IT staff have clear requirements to meet applicable compliance obligations.</li> <li>There is most likely a dedicated cybersecurity role or a small cybersecurity team.</li> </ul>	
<b>SP-CMM 3</b>	<ul style="list-style-type: none"> <li>There is a small IT staff that has clear requirements to meet applicable compliance obligations.</li> <li>There is likely a very competent leader (e.g., security manager / director) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.</li> </ul>	<ul style="list-style-type: none"> <li>IT staff have clear requirements to meet applicable compliance obligations.</li> <li>In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.).</li> <li>There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.</li> </ul>	
<b>SP-CMM 4</b>	It is unrealistic for a small organization to attain this level of maturity.	<ul style="list-style-type: none"> <li>IT staff have clear requirements to meet applicable compliance obligations.</li> <li>In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.).</li> <li>There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.</li> <li>Business stakeholders are made aware of the status of the cybersecurity and privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). Situational awareness is made possible through detailed metrics.</li> </ul>	
<b>SP-CMM 5</b>	It is unrealistic for a small or medium organization to attain this level of maturity.		<ul style="list-style-type: none"> <li>IT staff have clear requirements to meet applicable compliance obligations.</li> <li>In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC analysts, privacy, etc.).</li> <li>There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.</li> <li>Business stakeholders are made aware of the status of the cybersecurity and privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). Situational awareness is made possible through detailed metrics.</li> <li>The organization has a very aggressive business model that requires not only IT, but its cybersecurity and privacy practices, to be innovative to the point of leading the industry in how its products and services are designed, built or delivered.</li> <li>The organization invests heavily into developing AI/ML technologies to made near real-time process improvements to support the goal of being an industry leader.</li> </ul>



### **CMM 0 – NOT PERFORMED**

This level of maturity is defined as “non-existence practices,” where the control is not being performed.

- There are no identifiable work products of the process.

CMM 0 practices, or a lack thereof, are generally considered to be negligent. The reason for this is if a control is reasonably-expected to exist, by not performing the control that would be negligent behavior. The need for the control could be due to a law, regulation or contractual obligation (e.g., client contract or industry association requirement).

### **CMM 1 – PERFORMED INFORMALLY**

This level of maturity is defined as “ad hoc practices,” where the control is being performed, but lacks completeness & consistency.

- Base practices of the process area are generally performed.
- The performance of these base practices may not be rigorously planned and tracked.
- Performance depends on individual knowledge and effort.
- There are identifiable work products for the process.

CMM 1 practices are generally considered to be negligent. The reason for this is if a control is reasonably-expected to exist, by only implementing ad-hoc practices in performing the control that could be considered negligent behavior. The need for the control could be due to a law, regulation or contractual obligation (e.g., client contract or industry association requirement).

*Note – The reality with a CMM 1 level of maturity is often:*

- *For smaller organizations, the IT support role only focuses on “break / fix” work or the outsourced IT provider has a limited scope in its support contract.*
- *For medium / large organizations, there is IT staff but there is no management focus to spend time on the control.*

### **CMM 2 – PLANNED & TRACKED**

This level of maturity is defined as “requirements-driven practices,” where the expectations for controls are known (e.g., statutory, regulatory or contractual compliance obligations) and practices are tailored to meet those specific requirements.

- Performance of the base practices in the process area is planned and tracked.
- Performance according to specified procedures is verified.
- Work products conform to specified standards and requirements.

CMM 2 practices are generally considered to be “audit ready” with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control. CMM 2 practices are generally targeted on specific systems, networks, applications or processes that require the control to be performed for a compliance need (e.g., PCI DSS, HIPAA, NIST 800-171, etc.).

It can be argued that CMM 2 practices focus more on compliance over security. The reason for this is the scoping of CMM 2 practices are narrowly-focused and are not organization-wide.

*Note – The reality with a CMM 2 level of maturity is often:*

- *For smaller organizations:*
  - *IT staff have clear requirements to meet applicable compliance obligations or the outsourced IT provider is properly scoped in its support contract to address applicable compliance obligations.*
  - *It is unlikely that there is a dedicated cybersecurity role and at best it is an additional duty for existing personnel.*
- *For medium / large organizations:*
  - *IT staff have clear requirements to meet applicable compliance obligations.*
  - *There is most likely a dedicated cybersecurity role or a small cybersecurity team.*

### **CMM 3 – WELL-DEFINED**

This level of maturity is defined as “enterprise-wide standardization,” where the practices are well-defined and standardized across the organization.

- Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes.
- Process is planned and managed using an organization-wide, standardized process.

CMM 3 practices are generally considered to be “audit ready” with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control. Unlike CMM 2 practices that are narrowly focused, CMM 3 practices are standardized across the organization.



It can be argued that CMM 3 practices focus on security over compliance, where compliance is a natural byproduct of those secure practices. These are well-defined and properly-scoped practices that span the organization, regardless of the department or geographic considerations.

*Note – The reality with a CMM 3 level of maturity is often:*

- *For smaller organizations:*
  - *There is a small IT staff that has clear requirements to meet applicable compliance obligations.*
  - *There is a very competent leader (e.g., security manager / director) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.*
- *For medium / large organizations:*
  - *IT staff have clear requirements to implement standardized cybersecurity & privacy principles across the enterprise.*
  - *In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC, privacy, etc.)*
  - *There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.*

#### **CMM 4 – QUANTITATIVELY CONTROLLED**

This level of maturity is defined as “metrics-driven practices,” where in addition to being well-defined and standardized practices across the organization, there are detailed metrics to enable governance oversight.

- Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance.
- Performance is objectively managed, and the quality of work products is quantitatively known.

CMM 4 practices are generally considered to be “audit ready” with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control, as well as detailed metrics enable an objective oversight function. Metrics may be daily, weekly, monthly, quarterly, etc.

*Note – The reality with a CMM 4 level of maturity is often:*

- *For smaller organizations, it is unrealistic to attain this level of maturity.*
- *For medium / large organizations:*
  - *IT staff have clear requirements to implement standardized cybersecurity & privacy principles across the enterprise.*
  - *In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC, privacy, etc.)*
  - *There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.*
  - *Business stakeholders are made aware of the status of the cybersecurity and privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). This situational awareness is made possible through detailed metrics.*

#### **CMM 5 – CONTINUOUSLY IMPROVING**

This level of maturity is defined as “world-class practices,” where the practices are not only well-defined and standardized across the organization, as well as having detailed metrics, but the process is continuously improving.

- Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization.
- Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies.

CMM 5 practices are generally considered to be “audit ready” with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control and incorporates a capability to continuously improve the process. This is where Artificial Intelligence (AI) and Machine Learning (ML) would exist, since AI/ML would focus on evaluating performance and making continuous adjustments to improve the process. However, AI/ML are not requirements to be CMM 5.

*Note – The reality with a CMM 5 level of maturity is often:*

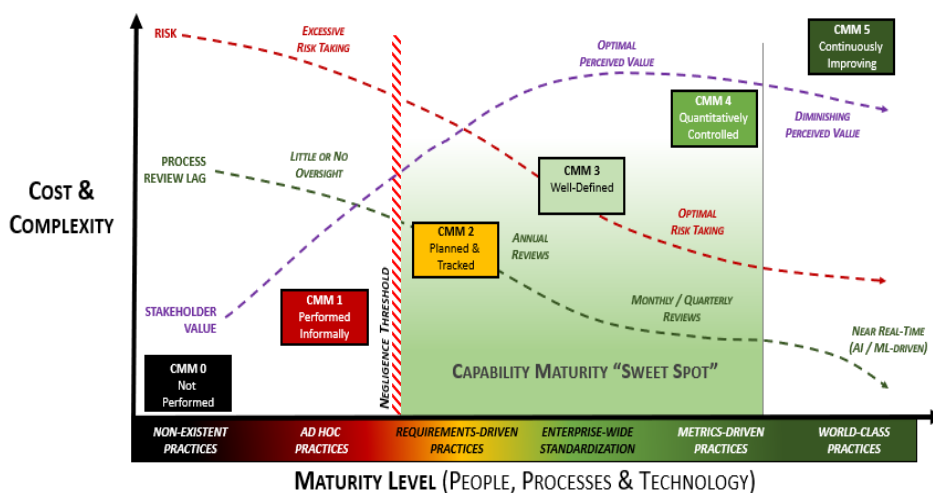
- *For smaller organizations, it is unrealistic to attain this level of maturity.*
- *For medium-sized organizations, it is unrealistic to attain this level of maturity.*
- *For large organizations:*

- *IT staff have clear requirements to implement standardized cybersecurity & privacy principles across the enterprise.*
- *In addition to the existence of a dedicated cybersecurity team, there are specialists (e.g., engineers, SOC analysts, GRC, privacy, etc.)*
- *There is a very competent leader (e.g., CISO) with solid cybersecurity experience who has the authority to direct resources to enact secure practices across the organization.*
- *Business stakeholders are made aware of the status of the cybersecurity and privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). This situational awareness is made possible through detailed metrics.*
- *The organization has a very aggressive business model that requires not only IT, but its cybersecurity and privacy practices, to be innovative to the point of leading the industry in how its products and services are designed, built or delivered.*
- *The organization invests heavily into developing AI/ML technologies to made near real-time process improvements to support the goal of being an industry leader.*

## DEFINING A CAPABILITY MATURITY “SWEET SPOT”

For most organizations, the “sweet spot” for maturity targets is between CMM 2 and 4 levels. What defines the ideal target within this zone is generally based on resource limitations and other business constraints, so it goes beyond just the cybersecurity and privacy teams dictating targets. Identifying maturity targets is meant to be a team effort between both technologists and business stakeholders.

From a business consideration, the increase in cost and complexity will always require cybersecurity and privacy leadership to provide a compelling business case to support any maturity planning needs. Speaking in terms the business can understand is vitally important.



*Note - During the development of the SP-CMM, a contributor identified an interesting insight that CMM 0-3 are “internal” maturity levels for cybersecurity and privacy teams, whereas CMM 4-5 are “external” maturity levels that expand beyond those teams. When you look at the stakeholders involved in CMM 0-3, it is almost entirely IT, cybersecurity and privacy. It isn’t until CMM 4-5 where there is true business stakeholder involvement in oversight and process improvement. This creates an internal to external shift in owning the cybersecurity & privacy program.*

## NEGLIGENCE CONSIDERATIONS

Without the ability to demonstrate evidence of both due care and due diligence, an organization may be found negligent. In practical terms, the “negligence threshold” is between CMM 1 and CMM 2. The reason for this is at CMM 2, practices are formalized to the point that documented evidence exists to demonstrate reasonable steps were taken to operate a control.

## RISK CONSIDERATIONS

Risk associated with the control in question decreases with maturity, but noticeable risk reductions are harder to attain above CMM 3. Oversight and process automation can decrease risk, but generally not as noticeably as steps taken to attain CMM 3.

## PROCESS REVIEW LAG CONSIDERATIONS

Process improvements increase with maturity, based on shorter review cycles and increased process oversight. What might have been an annual review cycle to evaluate and tweak a process can be near real-time with Artificial Intelligence (AI) and Machine Learning (ML).

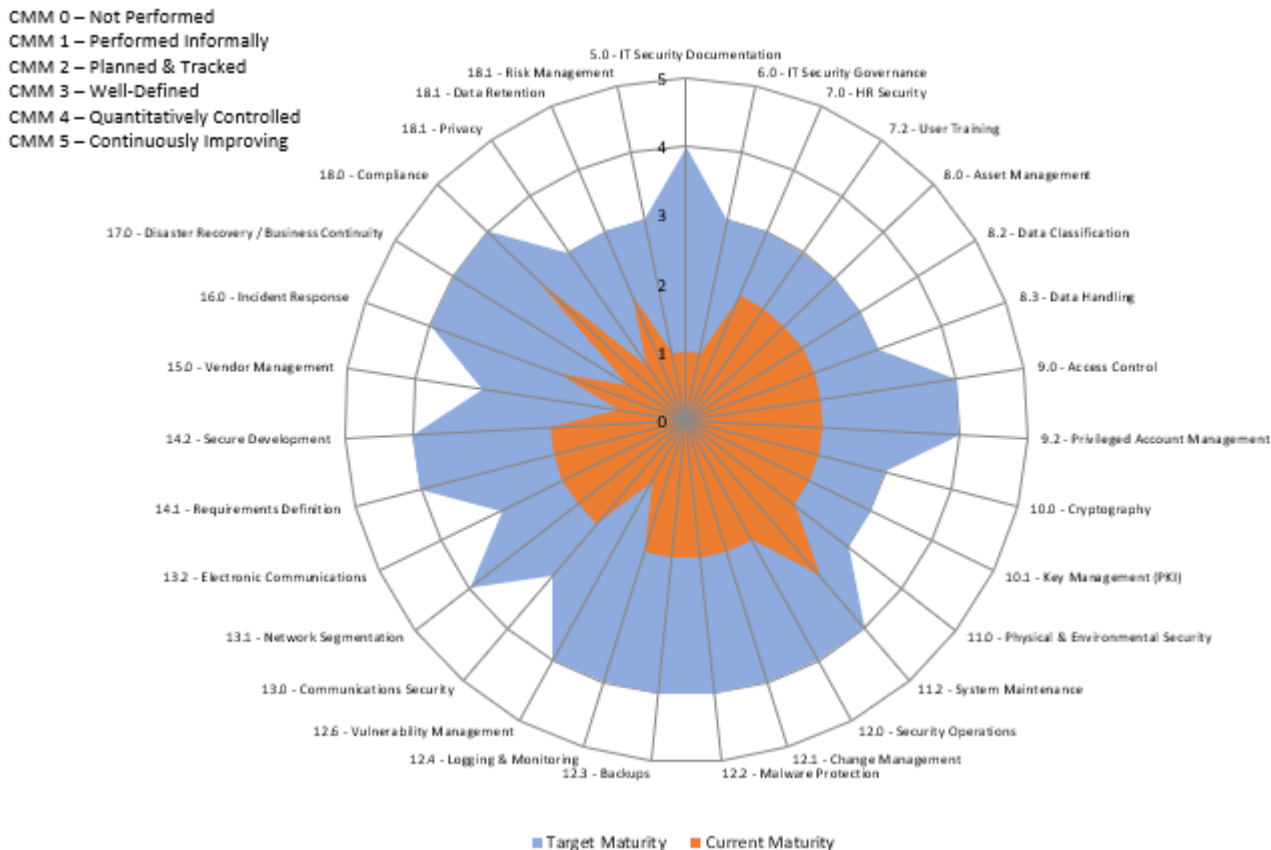
## STAKEHOLDER VALUE CONSIDERATIONS

The perceived value of security controls increases with maturity. However, perceived value tends to decrease after CMM 3 since the value of the additional cost and complexity becomes harder to justify to business stakeholders. Companies that are genuinely focused on being industry leaders are ideal candidates for CMM 5 targets to support their aggressive business model needs.

## SP-CMM USE CASE #1 – OBJECTIVE CRITERIA TO BUILD A CYBERSECURITY & PRIVACY PROGRAM

Identifying a target maturity state is intended to support your organization’s mission and strategy so without first understanding the broader mission of the organization and having prioritized objectives, a CISO/CIO/CPO will be guessing when it comes to establishing expectations for capability maturity. Like anything in life, if you fail to plan you plan to fail - CMM rollouts are no exception.

The time to execute a business plan to mature a cybersecurity and privacy program generally spans several years, where certain capabilities are prioritized over other capabilities. This means the CISO/CIO/CPO will establish CMM targets that evolve each year, based on prioritization. In the graphic below, the use of a spider chart can be beneficial to identify current vs future gaps with the SP-CMM. Prioritization of capability maturities may be based on risk assessments, audits, compliance obligations or management direction.



### IDENTIFYING THE PROBLEM

Using a CMM helps organizations avoid “moving targets” for expectations. Maturity goals define “what right looks like” in terms of the required people, processes and technology that are expected to exist in order to execute controls at the individual contributor level. Without maturity goals, it is very difficult and subjective to define success for a security & privacy program.

All too often, unprincipled cybersecurity & privacy leaders manipulate the business through Fear, Uncertainty and Doubt (**FUD**) to scare other technology and business leaders into supporting cybersecurity initiatives. These bad actors maintain the illusion of a strong cybersecurity & privacy program, when in reality the department is an array of disjointed capabilities that lacks a unifying plan. These individuals stay in the job long enough to claim small victories, implement some cool technology, and then jump ship for larger roles in other organizations to extend their path of disorder. In these cases, a common theme is the lack of viable business planning beyond a shopping list of technologies and headcount targets to further their career goals.

### CONSIDERATIONS

Cybersecurity & privacy departments are a cost center, not a revenue-generating business function. That means cybersecurity & privacy compete with all other departments for budget, and it necessitates a compelling business case to justify needed technology and staffing. Business leaders are getting smarter on the topic of cybersecurity & privacy, so these leaders need to rise above the FUD mentality and deliver value that is commensurate with the needs of the business.

When identifying a target level of maturity, it is crucial to account for your organization's culture. The reason for this is the implementation of perceived "draconian" levels of security can cause a revolt in organizations not accustomed to heavy restrictions. One good rule of thumb when deciding between CMM 3 and CMM 4 targets is this simple question: **"Do you want to be in an environment that is in control or do you want to be in a controlled environment?"** CMM 3 maturity is generally considered "an environment that is in control" where it is well-managed, whereas being in a CMM 4 environment is more of a "controlled environment" that is more controlled and less free. Given those considerations, environments not used to heavy restrictions may want to target CMM 3 as the highest-level of maturity targets. Additionally, the cost to mature from a CMM 3-4 or CMM 4-5 could be hundreds of thousands to millions of dollars, so there is a very real cost associated with picking a target maturity level. This is again where having management support is crucial to success, since this is ultimately a management decision.

From a CISO/CIO/CPO perspective, identifying a target level of maturity is also very beneficial in obtaining budget and protecting their professional reputation. In cases where business leadership doesn't support reaching the proposed target level of maturity, the CISO/CIO/CPO at least has documentation to prove he/she demonstrated a defined resourcing need (e.g., CMM level to support a business need) and the request was denied. Essentially, this can help cover a CISO/CIO/CPO in case an incident occurs and blame is pointed. That is just the reality of life for anyone in a high-visibility leadership position and being able to deflect unwarranted criticism is professional reputation insurance.

While a CISO/CIO/CPO can stop at the domain level to target CMM levels, it is expected that they or their subordinates go through each of the corresponding SCF controls to then tag each control with the appropriate target CMM level. These control targets can then be assigned to managers and Individual Contributors (IC) to develop operational plans to reach those goals. Ideally, a quarterly status review is conducted to oversee the progress made towards reaching the target CMM levels.

## SP-CMM USE CASE #2 – ASSIST PROJECT TEAMS TO APPROPRIATELY PLAN & BUDGET SECURE PRACTICES

When you consider regulations such as the EU GDPR, there is an expectation for systems, applications and processes to identify and incorporate cybersecurity and privacy by default and by design. In order to determine what is appropriate and to evaluate it prior to "go live" it necessitates expectations for control maturity to be defined.

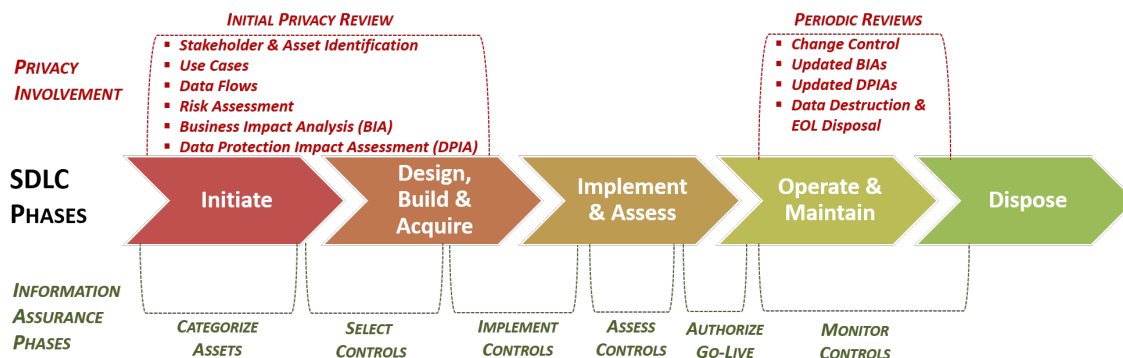
### IDENTIFYING THE PROBLEM

In planning a project or initiative, it is important to establish "what right looks like" from security and privacy controls that must be implemented to address all compliance needs. This includes internal requirements, as well as external requirements from applicable laws, regulations and contracts. Prior planning of requirements can reduce delays and other costs associated with re-engineering.

### CONSIDERATIONS

CMM 0-1 levels of maturity are identified as being deficient from a "reasonable person perspective" in most cases. Therefore, project teams need to look at the "capability maturity sweet spot" between CMM 2-4 to identify the reasonable people, processes and technologies that need to be incorporated into the solution.

As previously-covered, avoiding negligent behavior is a critical consideration. The most common constraints that impact a project's maturity are: (1) budget and (2) time. A System Development Life Cycle (SDLC) has constraints and the expectations are that security and privacy controls are applied throughout the SDLC.



Projects do not have unlimited budgets, nor do they tend to have overly flexible timelines that allow for new security & privacy tools to be installed and trained upon. From a project perspective, this is often going to limit target CMM levels to CMM 2-3 for planning purposes.

### **SP-CMM USE CASE #3 – PROVIDE OBJECTIVE CRITERIA TO EVALUATE THIRD-PARTY SERVICE PROVIDER SECURITY**

It is now commonplace for Third-Party Service Providers (TSPs), including vendors and partners, to be contractually bound to implement and manage a baseline set of cybersecurity and privacy controls. This necessitates oversight of TSPs to ensure controls are properly implemented and managed.

#### ***IDENTIFYING THE PROBLEM***

In managing a cybersecurity and privacy program, it is important to address controls in a holistic manner, which includes governing the supply chain. TSPs are commonly considered the “soft underbelly” for an organization’s security program, since TSP oversight has traditionally been weak or non-existent in most organizations. There have been numerous publicized examples of TSPs being the source of an incident or breach.

One of the issues with managing TSPs is most questionnaires ask for simple yes, no or not applicable answers. This approach lacks details that provide critical insights into the actual security posture of the TSP. The SP-CMM can be used to obtain more nuanced answers from TSPs by having those TSPs select from CMM 0-5 to answer if the control is implemented and how mature the process is.

#### ***CONSIDERATIONS***

CMM 0-1 levels of maturity are identified as being deficient from a “reasonable person perspective” in most cases. Therefore, organizations need to look at the “capability maturity sweet spot” between CMM 2-4 to identify the reasonable people, processes and technologies that need TSPs need to be able to demonstrate to properly protect your systems, applications, services and data, regardless of where it is stored, transmitted or processed. From a TSP management perspective, this is often going to limit target CMM levels to CMM 2-3 for most organizations.

TSP controls are expected to cover both your internal requirements, as well as external requirements from applicable laws, regulations and contracts. Using the SP-CMM can be an efficient way to provide a level of quality control over TSP practices. Being able to demonstrate proper cybersecurity and privacy practices is built upon the security principles of protecting the confidentiality, integrity, availability and safety of your assets, including data.





## 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

Risk Grouping	Risk #	Risk	Description of Possible Risk Due To Control Deficiency
Access Control	R-AC-1	Inability to maintain individual accountability	There is a failure to maintain asset ownership and it is not possible to have non-repudiation of actions or inactions.
	R-AC-2	Improper assignment of privileged functions	There is a failure to implement least privileges.
	R-AC-3	Privilege escalation	Access to privileged functions is inadequate or cannot be controlled.
	R-AC-4	Unauthorized access	Access is granted to unauthorized individuals, groups or services.
Asset Management	R-AM-1	Lost, damaged or stolen asset(s)	Asset(s) is/are lost, damaged or stolen.
	R-AM-2	Loss of integrity through unauthorized changes	Unauthorized changes corrupt the integrity of the system / application / service.
Business Continuity	R-BC-1	Business interruption	There is increased latency or a service outage that negatively impacts business operations.
	R-BC-2	Data loss / corruption	There is a failure to maintain the confidentiality of the data (compromise) or data is corrupted (loss).
	R-BC-3	Reduction in productivity	User productivity is negatively affected by the incident.
	R-BC-4	Information loss / corruption or system compromise due to technical attack	Malware, phishing, hacking or other technical attack compromise data, systems, applications or services.
	R-BC-5	Information loss / corruption or system compromise due to non-technical attack	Social engineering, sabotage or other non-technical attack compromises data, systems, applications or services.
Exposure	R-EX-1	Loss of revenue	A financial loss occurs from either a loss of clients or an inability to generate future revenue.
	R-EX-2	Cancelled contract	A contract is cancelled due to a violation of a contract clause.
	R-EX-3	Diminished competitive advantage	The competitive advantage of the organization is jeopardized.
	R-EX-4	Diminished reputation	Negative publicity tarnishes the organization's reputation.

	R-EX-5	Fines and judgements	Legal and/or financial damages result from statutory / regulatory / contractual non-compliance.
	R-EX-6	Unmitigated vulnerabilities	Unmitigated technical vulnerabilities exist without compensating controls or other mitigation actions.
	R-EX-7	System compromise	System / application / service is compromised affects its confidentiality, integrity, availability and/or safety.
Governance	R-GV-1	Inability to support business processes	Implemented security / privacy practices are insufficient to support the organization's secure technologies & processes requirements.
	R-GV-2	Incorrect controls scoping	There is incorrect or inadequate controls scoping, which leads to a potential gap or lapse in security / privacy controls coverage.
	R-GV-3	Lack of roles & responsibilities	Documented security / privacy roles & responsibilities do not exist or are inadequate.
	R-GV-4	Inadequate internal practices	Internal practices do not exist or are inadequate. Procedures fail to meet "reasonable practices" expected by industry standards.
	R-GV-5	Inadequate third-party practices	Third-party practices do not exist or are inadequate. Procedures fail to meet "reasonable practices" expected by industry standards.
	R-GV-6	Lack of oversight of internal controls	There is a lack of due diligence / due care in overseeing the organization's internal security / privacy controls.
	R-GV-7	Lack of oversight of third-party controls	There is a lack of due diligence / due care in overseeing security / privacy controls operated by third-party service providers.
	R-GV-8	Illegal content or abusive action	There is abusive content / harmful speech / threats of violence / illegal content that negatively affect business operations.
Incident Response	R-IR-1	Inability to investigate / prosecute incidents	Response actions either corrupt evidence or impede the ability to prosecute incidents.
	R-IR-2	Improper response to incidents	Response actions fail to act appropriately in a timely manner to properly address the incident.
	R-IR-3	Ineffective remediation actions	There is no oversight to ensure remediation actions are correct and/or effective.
	R-IR-4	Expense associated with managing a loss event	There are financial repercussions from responding to an incident or loss.
Situational Awareness	R-SA-1	Inability to maintain situational awareness	There is an inability to detect incidents.
	R-SA-2	Lack of a security-minded workforce	The workforce lacks user-level understanding about security & privacy principles.

## 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

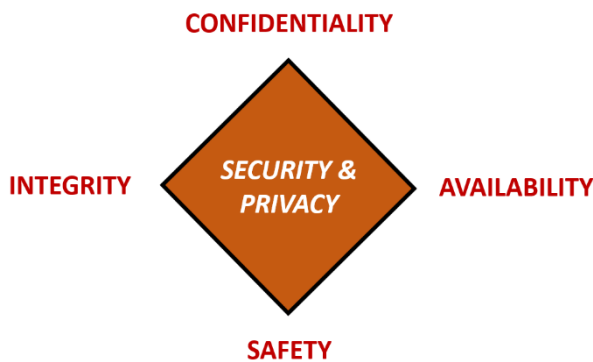
Manmade threats are caused by an element of human intent, negligence or error, or threat of violence that have the potential to impact individuals, processes, organizations or society, as a whole. The SP-RMM leverages a catalog of eleven (11) manmade threats:

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.

## 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.

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):

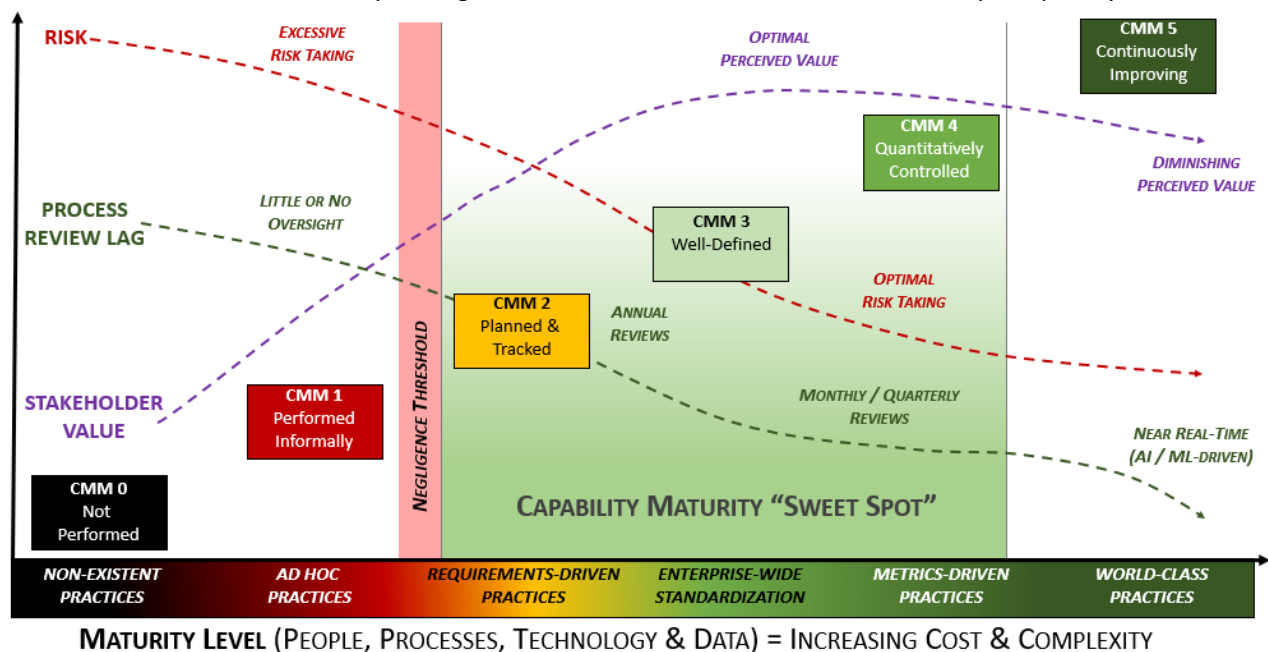


- **CONFIDENTIALITY** – This addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal privacy and proprietary information.
- **INTEGRITY** – This addresses protecting against improper modification or destruction, including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

*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 where the SP-CMM can be utilized 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:

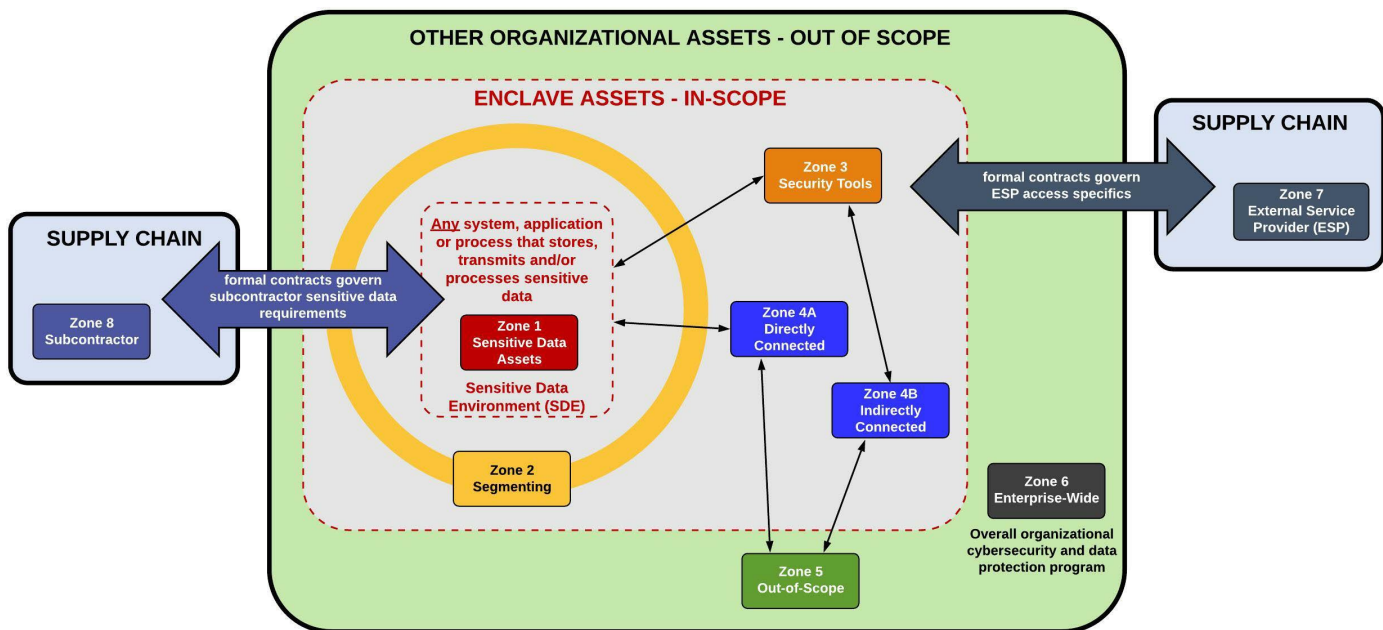
- Cybersecurity Risk Assessment
- Third-Party Risk Assessment
- Data Protection Impact Assessment (**DPIA**)
- Business Impact Assessment (**BIA**)
- Privacy Impact Assessment (**PIA**)

## 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 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.

Without specific statutory, regulatory or contractual scoping instructions, organizations can leverage the Unified Scoping Guide (**USG**) as the basis for scoping sensitive and/or regulated data.<sup>3</sup>



## 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.

<sup>3</sup> Unified Scoping Guide (USG) - <https://www.unified-scoping-guide.com/>

## 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

There are multiple methods to actually assess and calculate risk. 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, such as the matrix shown below:

SP-RMM Risk Matrix		Occurrence Likelihood					
		Remote [<1% chance of occurrence]	Highly Unlikely [1% to 10% chance of occurrence]	Unlikely [10% to 25% chance of occurrence]	Possible [25% to 70% chance of occurrence]	Likely [70% to 99% chance of occurrence]	Almost Certain [>99% chance of occurrence]
Risk Impact Effect	Catastrophic						EXTREME RISK
	Critical					SEVERE RISK	
	Major				HIGH RISK		
	Moderate		MODERATE RISK				
	Minor	LOW RISK					
	Insignificant						

## 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 such as:

- 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 [SP-RMM overview document](#).



### **13. PRIORITIZE & DOCUMENT RISKS**

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

- 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

## PRE-DEFINED CONTROL SETS

The SCF contains eight (8) pre-defined control sets to provide a starting point for certain functions to work from for applicable cybersecurity and data protection controls.

### BUSINESS MERGERS & ACQUISITIONS (SCF-B)

The SCF-B is a subset of the SCF that is tailored for evaluating the cybersecurity and privacy risks associated with Mergers & Acquisitions (M&A) due diligence. Due to the potentially complicated nature of the M&A evaluation, we designed the SCF-B to be comprehensive in nature. The following frameworks are leveraged to identify appropriate cybersecurity and privacy controls that should be evaluated as part of M&A due diligence activities:

- SOC2
- CIS CSC
- COBITv5
- COSO
- CSA CCM
- GAPP
- ISO 27002
- ISO 31000
- ISO 31010
- NIST 800-160
- NIST Cybersecurity Framework
- OWASP Top 10
- UL 2900-1
- EU GDPR

### EMBEDDED TECHNOLOGY CONTROLS (SCF-E)

The SCF-E is a subset of the SCF that is tailored for embedded technology (e.g., Internet of Things (IoT), Operational Technology (OT), Programmable Logic Controllers (PLCs), etc.) and is intended to assist companies with designing, building and maintaining secure processes, systems and applications.

### US GOVERNMENT CONTRACTOR CONTROLS (SCF-G)

The SCF-G is a subset of the SCF that is tailored for US government contractors that are in scope for NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC). The SCF-G is intended to assist US government contractors that have to comply with CMMC Level 3 and NIST SP 800-171 CUI & NFO controls.

### HEALTHCARE CONTROLS (SCF-H)

The SCF-H is a subset of the SCF that is tailored for the healthcare industry (e.g., HIPAA, NIST 800-53, etc.) and is intended to assist healthcare providers with designing, building and maintaining secure processes, systems and applications.

### CONTINUOUS MONITORING CONTROLS (SCF-M)

The SCF-M is a subset of the SCF that is tailored for maintaining situational awareness through continuous monitoring across your enterprise that range from system and network activity, to internal users, to vendors and other third-party service providers. The SCF-M is intended to assist companies with designing, building and maintaining processes, systems and applications that include both cybersecurity and privacy principles by default.

### PRIVACY CONTROLS (SCF-P)

The SCF-P is a subset of the SCF that is tailored for privacy (e.g., EU GDPR, ePrivacy Directive, FTC, etc.) and is intended to assist companies with designing, building and maintaining processes, systems and applications that include both cybersecurity and privacy principles by default. The SCF-P maps to the controls associated with the SCF Privacy Management Principles.

### RANSOMWARE PROTECTION CONTROLS (SCF-R)

The SCF-R is a subset of the SCF that is tailored for ransomware protection, based on based on NISTIR 8374 (draft). This highlights those controls that are associated with reducing risk associated with ransomware.

### **THIRD-PARTY RISK MANAGEMENT CONTROLS (SCF-T)**

The SCF-T is a subset of the SCF that is tailored for third-party risk (e.g., vendor risk management, supply chain risk, etc.) and is intended to assist companies with governing the third-party risks associated with the outsourced design, building and maintenance of processes, systems and applications.