SECURE CONTROLS FRAMEWORK

SCF OVERVIEW & PRACTITIONER GUIDEBOOK

version 2026.1

This document is designed for cybersecurity & data privacy practitioners to gain an understanding of:

- What the SCF is;
- What the SCF is not;
- The various capabilities of the SCF; and
- How the SCF is intended to be used in an organization.

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 data 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 https://securecontrolsframework.com

Table of Contents

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

Section 1. Terminology & Acronyms

The SCF Council recognizes two (2) primary sources for authoritative definitions for cybersecurity and data privacy terminology:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[1] and
- NIST Glossary.[2]

From the context of building a cybersecurity and data privacy program, it is important to clarify mandatory versus optional criteria:[3]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

Terminology Standardization

Within the cybersecurity profession, the term "control" can be applied to a variety of contexts and can serve multiple purposes. When used in content with the SCF, a control is a mechanism (e.g., a safeguard or countermeasure) designed to address protection needs specified by security requirements.

- Controls are:
  - The power to make decisions about how something is managed or how something is done;
  - The ability to direct the actions of someone or something;
  - An action, method or law that limits; and/or
  - A device or mechanism used to regulate or guide the operation of a machine, apparatus or system.
- Requirements are statements that translate, or express, a need and its associated constraints and conditions.

Additional clarification for assessment-relevant terminology:

- Assessment Boundary. The scope of an organization's control implementation to which assessment of objects is applied:
  - An assessment may involve multiple assessment boundaries; and
  - Assessment boundary may be defined as the People, Processes, Technologies, Data and/or Facilities (PPTDF) that comprise:
    - The entire organization;
    - A specific contract, project or initiative;
    - A specific Business Unit (BU) within an organization; or
    - A specific country, or geographic region, of the organization's business operations.
- Assessment Object. The item (e.g., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
- Control Inheritance: Security control inheritance is a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. [4]
- Material Control. When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data privacy control that:
  - It is not capable of having compensating controls; and
  - Its absence, or failure, exposes an organization to such a degree that it could have a material impact.
- Material Risk. When an identified risk poses a material impact, that is a material risk.

[1] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*

[2] *NIST Glossary - https://csrc.nist.gov/glossary*

[3] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*

[4] *NIST Glossary for Security Control Inheritance - https://csrc.nist.gov/glossary/term/security_control_inheritance*

-
    - A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
    - A material risk should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.
- Material Threat. When an identified threat poses a material impact, that is a material threat.
    - A material threat is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
    - A material threat should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.
- Material Incident. When an incident poses a material impact, that is a material incident.
    - A material incident is an occurrence that does or has the potential to:
        - Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the organization; and/or
        - Constitute a violation, or imminent threat of violation, of an organization's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).
    - Reasonably foreseeable material incidents should be documented in an organization's Incident Response Plan (IRP) that chronicles the organization's relevant and plausible incidents, so there are appropriate practices to identify, respond to and recover from such incidents.
- Material Weakness. A material weakness is a deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data privacy controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance.
    - When there is an existing deficiency (e.g., control deficiency) that poses a material impact, that is a material weakness (e.g., inability to maintain access control, lack of situational awareness to enable the timely identification and response to incidents, etc.).
    - A material weakness will be identified as part of a gap assessment, audit or other form of assessment as a finding due to one (1), or more, control deficiencies. A material weakness should be documented in an organization's Plan of Action & Milestones (POA&M), risk register, or similar tracking mechanism for remediation purposes.
- Mechanism. A mechanism can be described as a: [5]
    - Process or system that is used to produce a particular result; or
    - Device or method for achieving a security-relevant purpose.
- Reciprocity. Reciprocity is an agreement among participating organizations to accept each other's: [6]
    - Security assessments to reuse system resources; and/or
    - Assessed security posture to share information.
- Risk. A risk is:
    - A situation where someone, or something valued, is exposed to danger, harm or loss (noun); or
    - To expose someone or something valued to danger, harm or loss (verb).
- Risk Appetite: The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.[7]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potentially desired result. [8]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.[9]
- Threat. A threat:
    - Is a person, or thing, likely to cause damage or danger (noun); or
    - Indicates impending damage or danger (verb).

[5] *NIST Glossary for Mechanism - https://csrc.nist.gov/glossary/term/mechanism*

[6] *NIST Glossary for Reciprocity - https://csrc.nist.gov/glossary/term/reciprocity*

[7] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*

[8] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*

[9] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*

ACRONYMS

The following acronyms are defined as:

Acronym	Term	Definition
1PD	First Party Declaration	1PDs are self-attestations (e.g., internal assessments).
3PA	Third-Party Attestation	3PA are attestations made by an independent third-party, generally in the performance of an assessment or audit.
3PAAC	Third-Party Assessment, Attestation and Certification Services	Assessment, attestation and certification services performed by a third-party organization.
3PAO	Third-Party Assessment Organization	A company that performs assessment, attestation and certification services.
AAT	Artificial Intelligence and Autonomous Technologies	Tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.
AO	Assessment Objective	AOs are objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.
APIT	Automated Point In Time	APIT assessments utilize automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence: ▪ Relevant to a specific point in time (time at which the control was evaluated); ▪ In situations where technology cannot evaluate evidence, evidence is manually reviewed; and ▪ The combined output of automated and manual reviews of artifacts is used to derive a finding.
ATE	Assessment Technical Expert	ATE are assessment team members who have the necessary subject matters expertise to conduct a specific part of an assessment. ATE report to the ATL.
ATL	Assessment Team Lead	An ATL is an individual assigned by the 3PAO to lead its assessment team in the conduct of 3PAAC Services.
AEHR	Automated Evidence with Human Assessment	AEHR assessments are used for ongoing, continuous control assessments: ▪ AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and ▪ Recurring human reviews: ○ Evaluate the legitimacy of the results from automated control assessments; and ○ Validate the automated evidence review process to derive a finding.
CIAS	Confidentiality, Integrity, Availability and/or Safety	CIAS is an evolution of the "CIA Triad" concept that defines the purpose of security controls. It adds the component of Safety.
COI	Conflict of Interest	COI involves situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.
CPE	Continuing Professional Education	CPE describes the ongoing process of improving skills and competencies through formal or informal educational activities.
DSR	Discretionary Security Requirements	DSR are discretionary cybersecurity and/or data privacy controls that address voluntary industry practices or internal requirements. DSR are primarily internally influenced, based on the organization's respective industry and risk tolerance.
ERL	Evidence Request List	ERLs establish a finite list of supporting evidence used in an assessment: ▪ Prior to the start of the assessment, an ERL is provided by the 3PAO to the OSA. ▪ The ERL's standardized evidence expectations allow OSAs to have sufficient time to accumulate reasonable evidence to determine the adequacy of control design and operation.
ESP	External Service Provider	An independent, third-party organization that provides services, technologies, facilities and/or people. ESPs include but are not limited to: ▪ Consulting / professional services;

		▪ Software development; ▪ Staff augmentation; and ▪ Technology support (e.g., Managed Services Provider (MSP)).
MCR	Minimum Compliance Requirements	MCR are minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations.
MPIT	Manual Point In Time	MPIT assessments are a traditional assessment methodology: ▪ Relevant to a specific point in time (time at which the control was evaluated); and ▪ Relies on the manual review of artifacts to derive a finding.
MLC	Maturity Level Criteria	MLC are specific to each maturity level to define reasonable staffing, technologies and processes to implement the desired level of maturity.
MSA	Master Services Agreement	MSAs are comprehensive contracts between two parties that establish terms and conditions of current and future transactions.
OSA	Organization Seeking Assessment	A company, entity or business unit seeking the external assessment.
PbD	Privacy by Design	Data protection through the design and governance of processes and technologies. PbD prioritizes data protection as a core business requirement, rather than a technical feature.
RASCI	Responsible, Accountable, Supportive, Consulted & Informed	Refers to a RASCI matrix that defines responsibilities associated with individuals or teams: ▪ Responsible - entity directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task; ▪ Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - entity(ies) not involved in task execution but are informed when the task is completed.
ROC	Report on Conformity	A formalized report that issues an assessment conformity designation. The ROC summarizes the assessment findings and justification for the conformity designation.
SbD	Secure by Design	Processes and technologies are designed and built in a way that protects against reasonable threats. SbD prioritizes cybersecurity as a core business requirement, rather than treating it as a technical feature.
SOW	Statement of Work	SOWs are contracts that cover the work management aspects of a project (e.g., scope, timeline, cost, responsibilities, etc.).

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

SECTION 2. INTRODUCTION TO THE SECURE CONTROLS FRAMEWORK®

The Secure Controls Framework® (SCF) focuses on internal cybersecurity and data protection controls. These are the administrative, technical and physical controls (e.g., 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/or remediated. There is no cost to use the SCF and quite a few Governance, Risk and Compliance (GRC) platforms natively support the SCF as a built-in control set.

The SCF is a more efficient way to operationalize cybersecurity and data privacy operations by simplifying the underlying controls that comprise the basis of an organization's cybersecurity and data privacy program. The reality is that most organizations struggle with defining the minimum-security requirements that are necessary to address both (1) applicable compliance obligations and (2) the need for secure practices. The SCF provides a straightforward and scalable method to define those "must have" and "nice to have" requirements into a holistic control set to operationalize cybersecurity operations, risk management and third-party governance.

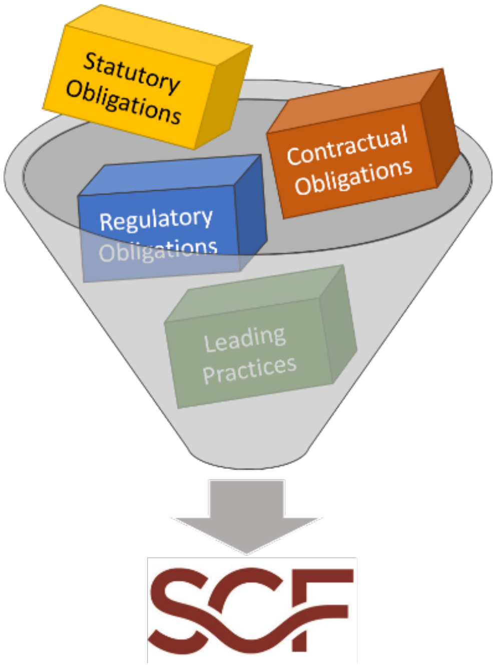
In simple terms, the SCF is a metaframework, a "framework of frameworks." It is a catalog of controls made up of over 200 authoritative sources (e.g., statutory, regulatory and contractual frameworks). This controls catalog contains over 1,200 controls and is logically organized into thirty-three (33) domains. The structure of the SCF normalizes disparate control language into something that is usable across technology, cybersecurity, data privacy and other departments where they can share the same control language. The SCF enables not only intra-organization standardization, but inter-organization standardization (e.g., control GOV-03 means the same thing to one organization to any other organization using the SCF). 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.

The SCF is made up of volunteers who are specialists within the cybersecurity and data privacy professions. These people are seasoned auditors, engineers, architects, incident responders, consultants and other specialists who live and breathe these topics on a daily basis. The end product of their labor is "expert-derived content" that makes up the SCF.

WHY SHOULD AN ORGANIZATION 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 or two (1 or 2) compliance requirements, the SCF might be considered overkill for your needs. However, for companies that have three or more (3+) compliance requirements (e.g., organization that has requirements to address NIST 800-171, NIST CSF, SOC 2 and GDPR), then the SCF is a great tool to streamline the management of disparate cybersecurity & data privacy control frameworks.

In developing the SCF, we identified and analyzed over 200 cybersecurity and data protection laws, regulations and frameworks. Through analyzing these thousands of legal, regulatory and framework requirements, we identified the commonalities, and this allows several thousand unique controls to be addressed by approximately 1,200 controls that make up 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.



EXPERT INSIGHT (CONTROL SELECTION CONSIDERATIONS): Some people who are new to the SCF freak out due to their misunderstanding where they think they have to all 1,200+ controls in the SCF. That is just not the case. It is best to visualize the SCF as a "buffet of cybersecurity & data privacy controls," where the presented buffet is a selection of 1,200+ controls. Just as you do not eat everything possible on a buffet table, the same applies to the SCF's control set where you only select the controls you need. 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 concept of tailoring the control set is explained at the end of this section.

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 & data 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 & data privacy controls so that the same controls can be used among companies and teams (e.g., privacy, cybersecurity, IT, project, procurement, etc.); and
- 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

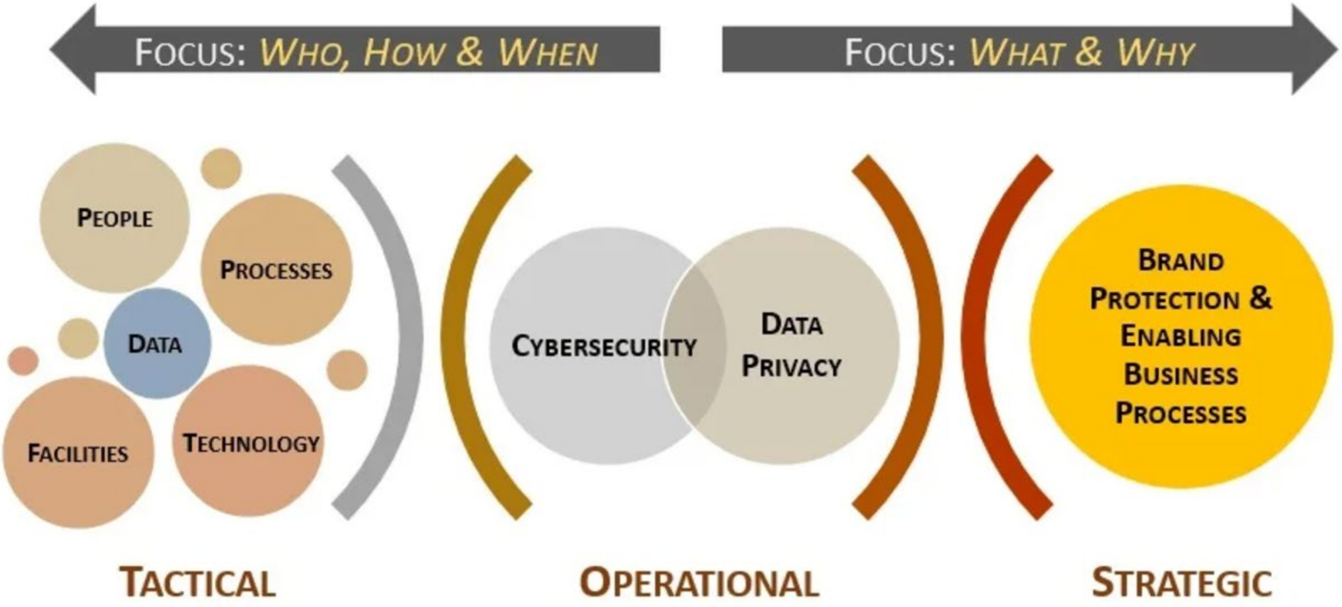
While the SCF is a comprehensive catalog of controls that is designed to enable companies to design, build and maintain secure processes, systems and applications, the SCF will only ever be a control set and is not a "magic bullet" technology solution to address every possible cybersecurity & data privacy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

The SCF is not:

- A substitute for performing due diligence and due care to understand and manage your specific compliance needs;
- A complete technology or documentation solution to address all your cybersecurity & data privacy needs (e.g., the policies, standards, procedures and processes you need to have in place to be secure and compliant); and
- 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.

Addressing The Who? What? Where? When? Why? and How?

Ideally, the SCF can be used to address the "who, what where, when, why and how" for cybersecurity and data privacy at the strategic, operational and tactical levels within your organization!

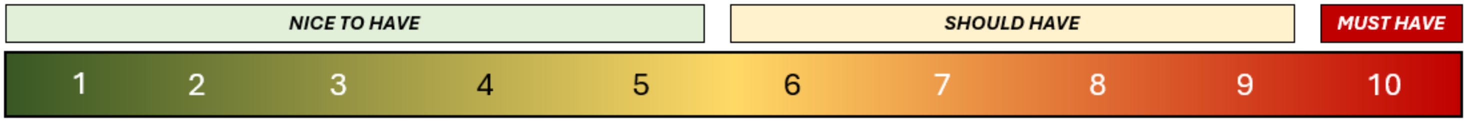


Using the SCF should be viewed as a long-term tool to not only help with compliance-related efforts but to ensure cybersecurity & data privacy principles are properly designed, implemented and maintained. The SCF helps implement a holistic approach to protecting the Confidentiality, Integrity, Availability 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.

SCF Control Weighting Explanation

The SCF assigns a value on a scale from 1-10, with 1 being the least important and 10 being the most important. These values are subjective, based on SCF contributor discussion, since control weighting is important to help prioritize controls and assist with the understanding what really matters from a risk management perspective. For an insight into the thought process, a control weighting of 10 was framed as *"Would you do business with an organization that did not have this control in place?"* where certain controls were identified as an absolute minimum from a risk threshold perspective from a "reasonable person" perspective.

- Those controls designated as a score of **10** should be considered a **MATERIAL / KEY CONTROL** (e.g., lack of or a deficiency should be considered a material weakness).
- On the opposite side of the spectrum, a score of **1** was deemed **"nice to have"** but did not materially affect risk.



EXPERT INSIGHT (MATERIALITY): *The intended usage of materiality is meant to provide relevant context regarding risk thresholds. Materiality designations are intended to act as a "guard rail" for risk management decisions. A material weakness crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk. A financial benchmark is commonly used to determine materiality. From a financial impact perspective, for an item to be considered material, the control deficiency, risk, threat or incident (singular or a combination) generally must meet one, or more, of the following criteria where the potential financial impact is measured as:*[10]

- *≥ 5% of pre-tax income*
- *≥ 0.5% of total assets*
- *≥ 1% of total equity (shareholder value); and/or*
- *≥ 0.5% of total revenue.*

Tailoring Is Required - Not All SCF Controls Are Applicable To Your Organization

The SCF is a tool and is only as good as how it is used – just like a pocketknife shouldn't be used as a prybar. If a SCF user incorrectly scopes their requirements, the resulting controls will not address their applicable compliance requirements. That is not a deficiency of the SCF – that is simply negligence on the part of the user of the tool.

To ensure scoping is done properly, it is imperative for you to speak with your legal, IT, project management, cybersecurity and procurement teams. 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 this list of requirements will then make it simple to go through and customize the SCF for your specific needs!

Understanding the requirements for both cybersecurity & data 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.

Beyond just using compliance terminology properly, understanding which of the three types of compliance is crucial in managing both Secure, Compliant & Resilient Risk within an organization. The difference between non-compliance can be as stark as (1) going to jail, (2) getting fined, (3) getting sued, (4) losing a contract or (5) an unpleasant combination of the previous options.

Understanding the "hierarchy of pain" with compliance leads to well-informed risk decisions that influence technology purchases, staffing resources and management involvement. That is why it serves both cybersecurity and IT professionals well to understand the compliance landscape for their benefit, since presenting issues of non-compliance in a compelling business context to get the resources needed to complete their jobs.

The most common types of compliance requirements are:

1. Statutory;
2. Regulatory; or
3. Contractual.

[10] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*

Statutory Requirements

Statutory obligations are required by law and refer to current laws that were passed by a state or federal government. These laws are generally static and rarely change unless a new law is passed that updates it (e.g., HITECH Act, provided updates to HIPAA, CPRA provided updates to CCPA, etc.).

From a cybersecurity & data privacy perspective, statutory compliance examples include but are not limited to:

- **US – Federal Laws**
    - Children's Online Privacy Protection Act (COPPA)
    - Fair and Accurate Credit Transactions Act (FACTA) – including "Red Flags" rule
    - Family Education Rights and Privacy Act (FERPA)
    - Federal Information Security Management Act (FISMA)
    - Federal Trade Commission (FTC) Act
    - Gramm-Leach-Bliley Act (GLBA)
    - Health Insurance Portability and Accountability Act (HIPAA) / HITECH Act
    - Sarbanes-Oxley Act (SOX)
- **US – State Laws**
    - California SB1386
    - Massachusetts 201 CMR 17.00
    - Oregon ORS 646A.622
- **International Laws**
    - Canada – Personal Information Protection and Electronic Documents Act (PIPEDA)
    - UK – Data Protection Act (DPA)
    - Other countries' variations of Personal Data Protect Acts (PDPA)

Regulatory Requirements

Regulatory obligations are required by law, but they are different from statutory requirements in that these requirements refer to rules issued by a regulating body that is appointed by a state or federal government. These are legal requirements through proxy, where the regulating body is the source of the requirement. It is important to keep in mind that regulatory requirements tend to change more often than statutory requirements.

From a cybersecurity & data privacy perspective, regulatory compliance examples include but are not limited to:

- **US Regulations**
    - Defense Federal Acquisition Regulation Supplement (DFARS) (NIST 800-171)
    - Federal Acquisition Regulation (FAR)
    - Federal Risk and Authorization Management Program (FedRAMP)
    - DoD Information Assurance Risk Management Framework (DIARMF)
    - National Industrial Security Program Operating Manual (NISPOM)
    - New York Department of Financial Services 23 NYCRR 500
- **International Regulations**
    - European Union General Data Protection Regulation (EU GDPR)

Contractual Requirements

Contractual obligations are required by legal contracts between private parties. This may be as simple as a cybersecurity or privacy addendum in a vendor contract that calls out unique requirements, but it also includes broader requirements from an industry association that membership brings certain obligations.

From a cybersecurity & data privacy perspective, common contractual compliance examples include but are not limited to:

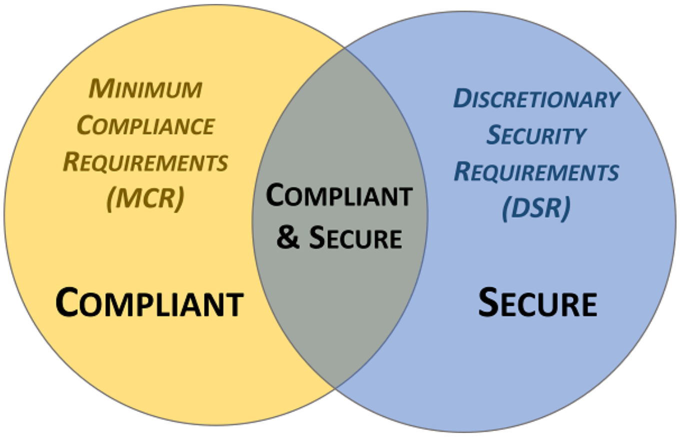
- Cybersecurity Supply Chain Risk Management (C-SCRM) (e.g., NIST SP 800-161 R1)
- Payment Card Industry Data Security Standard (PCI DSS)
- Service Organization Control (SOC)
- Generally Accepted Privacy Principles (GAPP)
- Center for Internet Security (CIS) Critical Security Controls (CSC)
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

Tailoring SCF Controls - Defining “Must Have” vs “Nice To Have” Controls

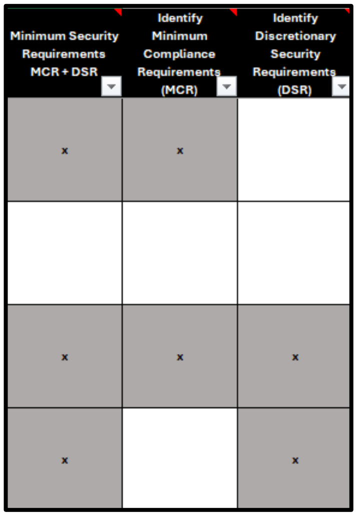
Secure and compliant operations exist when applicable controls are properly scoped and implemented. To assist in this process, an organization’s applicable controls should be categorized according to “must have” vs “nice to have” requirements:

- Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- Discretionary Security Requirements (DSR) are tied to the organization’s risk appetite since DSR are “above and beyond” MCR, where the organization self-identifies additional cybersecurity & data privacy controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments. DSR are primarily internally-influenced, based on the organization’s respective industry and risk tolerance. While MCR establishes the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.


Minimum Compliance Requirements (MCR)
Compliant
Compliant & Secure
Discretionary Security Requirements (DSR)
Secure

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

Within the SCF, there is a column labelled “Minimum Security Requirements (MSR) MCR + MSR” that will assist you in this process.



Minimum Security Requirements MCR + DSR	Identify Minimum Compliance Requirements (MCR)	Identify Discretionary Security Requirements (DSR)
x	x	
x	x	x
x		x

Follow these steps to tailor the SCF:

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).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).
2. A selection of either MCR or DSR will automatically select the MSR + DSR column:
   a. In the MCR column, simply put an “x” to mark that control as being “must have” controls.
   b. In the DSR column, simply put an “x” to mark that control as being “nice to have” controls.
3. Unfilter the column you just performed this task on and do it to the next law, regulation or framework that you need to map.
4. Repeat steps 2 and step 3 until all your applicable laws, regulations and frameworks are mapped to.

EXPERT INSIGHT (BASELINING): The MSR + DSR resulting column shows the SCF controls that considered an organization's Minimum Security Requirements (MSR) that will be used. The MSR is the baseline set of controls the organization should implement to be both secure and compliant.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

SECTION 3. SCF TRAINING & INDIVIDUAL CERTIFICATIONS

There is individual-level training and SCF certifications available at https://training.securecontrolsframework.com. The four (4) individual certifications are:

SCF PRACTITIONER

SCF Practitioners are certified individuals who have the knowledge and skills to: [11]

1. implement SCF controls that align with the SCF recommended practices and structure; and
2. maintain an organization's cybersecurity and data protection program.

SCF ARCHITECT

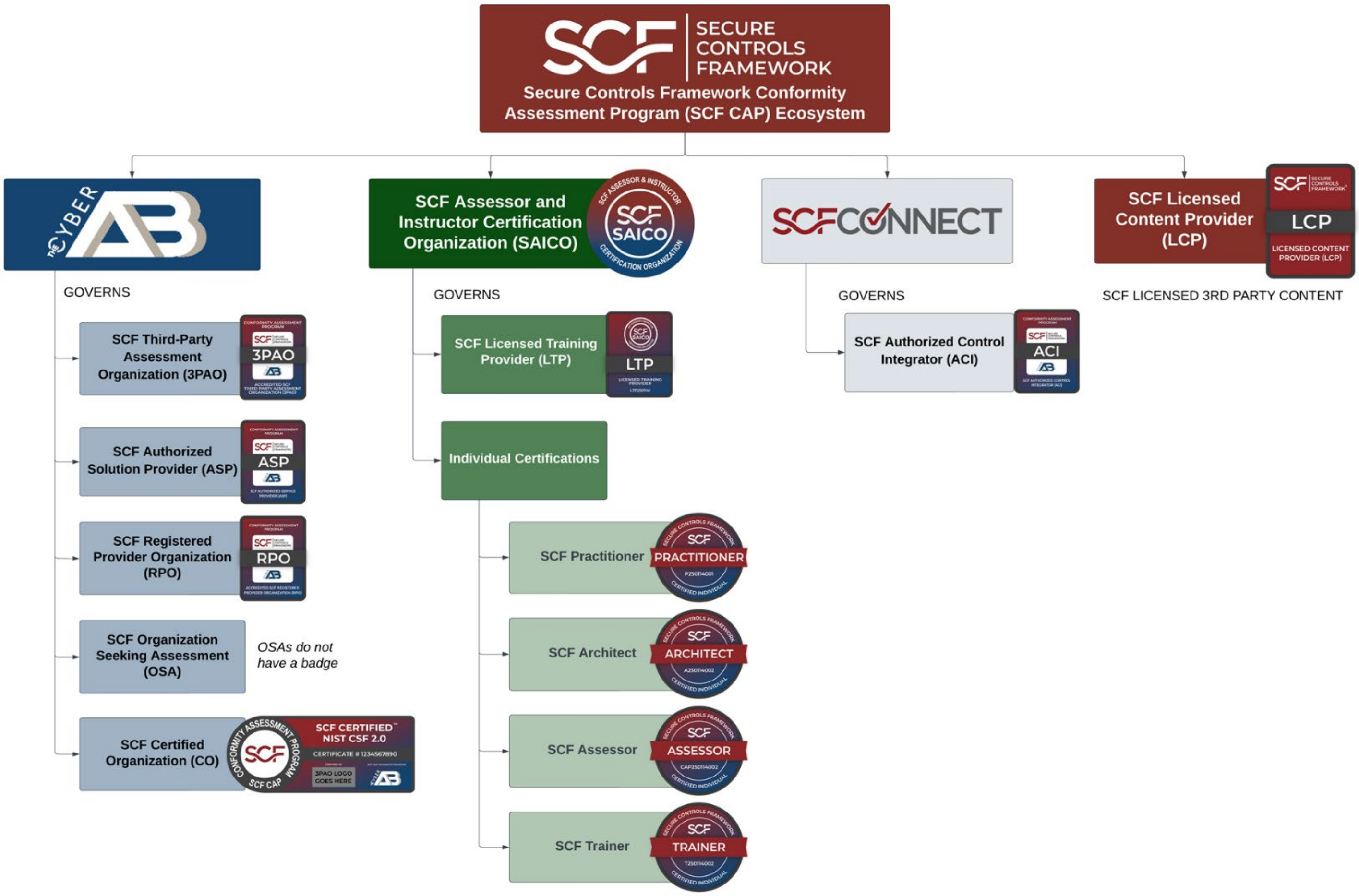
SCF Architects are certified individuals who have the knowledge and skills to design SCF-based cybersecurity and data protection programs that are capable of addressing the tactical, operational and strategic needs of the organization specific to its unique People, Processes, Technologies, Data and Facilities (PPTDF) considerations.[12]

SCF ASSESSOR

SCF Assessors are certified individuals who work for a SCF Third-Party Assessment Organization (3PAO) to perform conformity assessments as part of the SCF's Conformity Assessment Program (SCF CAP).[13]

SCF TRAINER

SCF Trainers are certified individuals who work for a SCF Licensed Training Provider (LTP) to perform SCF-approved training. The SCF Trainer role is expected to be available in 2025.


SCF SECURE CONTROLS FRAMEWORK
Secure Controls Framework Conformity Assessment Program (SCF CAP) Ecosystem
THE CYBER AB
GOVERNS
SCF Third-Party Assessment Organization (3PAO)
3PAO
SCF Authorized Solution Provider (ASP)
ASP
SCF Registered Provider Organization (RPO)
RPO
SCF Organization Seeking Assessment (OSA)
OSAs do not have a badge
SCF Certified Organization (CO)
SCF CERTIFIED NIST CSF 2.0
CERTIFICATE # 1234567890
3PAO LOGO GOES HERE
SCF CAP
SCF Assessor and Instructor Certification Organization (SAICO)
SCF SAICO
GOVERNS
SCF Licensed Training Provider (LTP)
LTP
Individual Certifications
SCF Practitioner
PRACTITIONER
SCF Architect
ARCHITECT
SCF Assessor
ASSESSOR
SCF Trainer
TRAINER
SCFCONNECT
GOVERNS
SCF Authorized Control Integrator (ACI)
ACI
SCF Licensed Content Provider (LCP)
LCP
LICENSED CONTENT PROVIDER (LCP)
SCF LICENSED 3RD PARTY CONTENT

[11] SCF Practitioner training - https://training.securecontrolsframework.com/products/courses/scf-practitioner-training

[12] SCF Architect training - https://training.securecontrolsframework.com/products/courses/scf-architect-training

[13] SCF Assessor training - https://training.securecontrolsframework.com/products/courses/scf-assessor-training

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

SECTION 4. DESIGNING & BUILDING AN AUDIT-READY CYBERSECURITY & DATA PRIVACY PROGRAM

Building an audit-ready cybersecurity & data privacy program requires addressing the holistic nature of cybersecurity & data privacy concerning how People, Processes, Technologies, Data & Facilities (PPTDF) impact security practices.

Building a security program that routinely incorporates cybersecurity & data protection practices into daily operations requires a mastery of the basics. A useful analogy is with LEGO®, the children's toy. With LEGO® you can build nearly anything you want, but it starts with the understanding of the various LEGO® shapes and how they either snap together or are incompatible.

- Mastering the fundamentals of LEGO® building enables someone to become immensely creative since that individual knows how everything interacts. It becomes possible to either follow the instructions or design and build structures based on their own imagination.
- Conversely, when an individual ignores the fundamental concepts with LEGO® building, any created structure will be weak and include systemic flaws.

Cybersecurity and data privacy controls are not much different from LEGO® blocks, 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 cybersecurity or data privacy "best practice" is a LEGO® block, it is possible to conceptualize how certain requirements are the foundation that form the basis for other components to attach to. Only when all the building blocks come together and take shape do you get a functional security / privacy program!

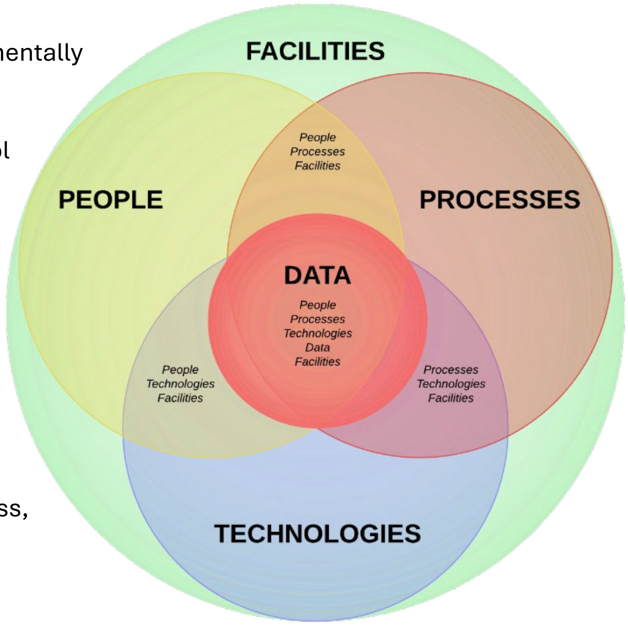
Think of the SCF as a toolkit for you to build out your overall security program domain-by-domain so that cybersecurity & data privacy principles are designed, implemented and managed by default!

PEOPLE, PROCESSES, TECHNOLOGY, DATA & FACILITIES (PPTDF)

The concept is to address the broader PPTDF that are what controls fundamentally exists to govern.

The PPTDF model provides a comprehensive approach to address control applicability. These five (5) components provide a lens to view the applicability of controls:

1. People – Applicable to humans (e.g., training, background checks, non-disclosure agreements, etc.).
2. Processes – Applicable to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).
3. Technology – Applicable to systems, applications and services (e.g., secure baseline configurations, patching, etc.).
4. Data – Applicable to data protection (e.g., encrypting sensitive/regulated data, applying metatags, etc.).
5. Facilities – Applicable to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).



HOLISTIC APPROACH TO ADDRESS CONTROL APPLICABILITY

Cybersecurity practitioners generally agree that the importance of robust cybersecurity and data protection controls cannot be overstated. However, the applicability of those controls is sometimes in question since not all controls are applicable. To help demonstrate the applicable nature of controls:

- An employee cannot have a secure baseline configuration applied;
- An Incident Response Plan (IRP) cannot sign a Non-Disclosure Agreement (NDA), use Multi-Factor Authentication (MFA) or be patched;
- You cannot apply end user training to a firewall;
- Sensitive / regulated data cannot be assigned roles and responsibilities; and
- Your data center cannot undergo employee background screening.

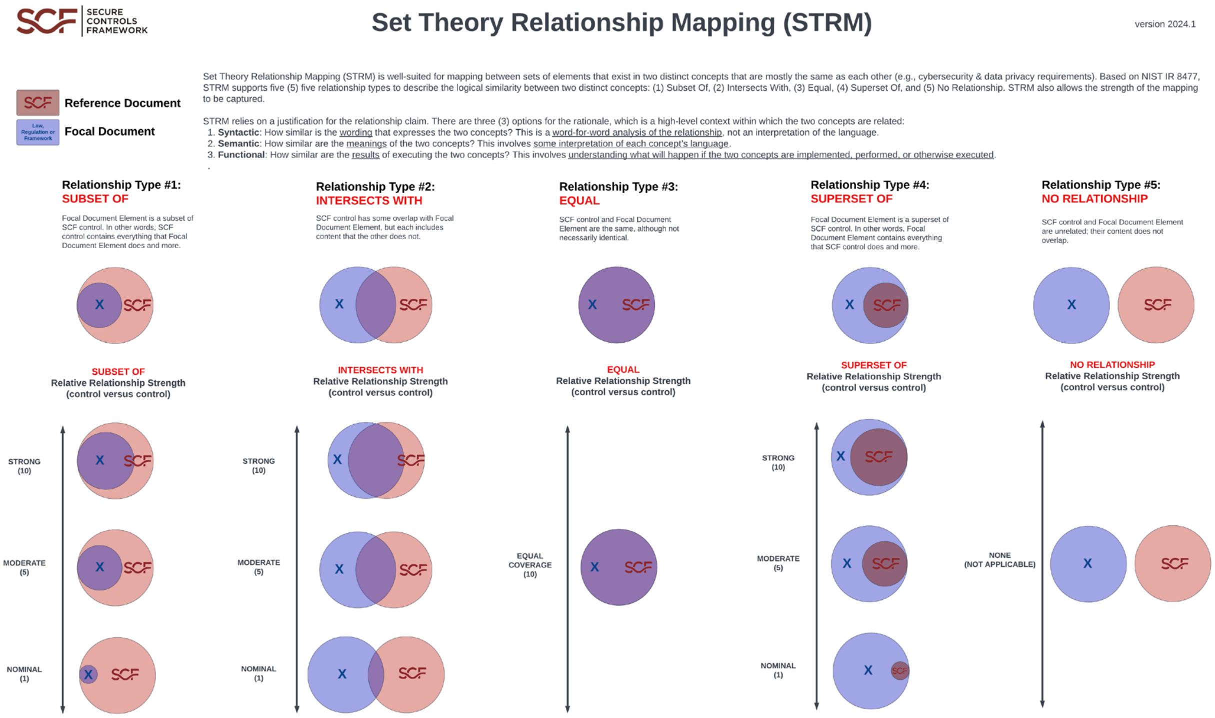
NIST IR 8477 - Set Theory Relationship Mapping (STRM)

Starting in 2024, the SCF began leveraging the Set Theory Relationship Mapping (STRM) for crosswalk mapping. STRM is generally well-suited to evaluate cybersecurity and data privacy laws, regulations and frameworks. With the publishing of NIST IR 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and data privacy Concept Mappings* it establishes the US Government's playbook for how to perform crosswalk mapping between different cybersecurity and data privacy laws, regulations and frameworks.[14]

NIST IR 8477 is part of NIST's broader NIST OLIR Program that is an *"effort to facilitate Subject Matter Experts (SMEs) in defining standardized online informative references (OLIRs) between elements of their documents, products, and services and elements of NIST documents…"* The SCF currently participates in the National Online Informative References (OLIR) Program and with NIST's preference for STRM, we decided an aligned crosswalk mapping methodology makes sense.[15]

For SCF's STRM practices, the SCF is always the "reference document" and the law, regulation or framework being mapped to is always the "focal document."

REFERENCE DOCUMENT (RD) **FOCAL DOCUMENT (FD)**



Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts: (1) Subset Of, (2) Intersects With, (3) Equal, (4) Superset Of, and (5) No Relationship. STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

.

Relationship Type #1: SUBSET OF — Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

Relationship Type #2: INTERSECTS WITH — SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

Relationship Type #3: EQUAL — SCF control and Focal Document Element are the same, although not necessarily identical.

Relationship Type #4: SUPERSET OF — Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

Relationship Type #5: NO RELATIONSHIP — SCF control and Focal Document Element are unrelated; their content does not overlap.

More information and graphics can be viewed at:
https://securecontrolsframework.com/content/strm/scf-set-theory-relationship-mapping.pdf

[14] *NIST IR 8477 - https://csrc.nist.gov/pubs/ir/8477/final*
[15] *SCF NIST OLIR Participation - https://securecontrolsframework.com/nist-olir-participation/*

STRM Relationship Types

Within STRM, there are five (5) relationship types:

1. Subset Of;
2. Intersects With;
3. Equal;
4. Superset Of; and
5. No Relationship.

STRM Relationship Type #1: SUBSET OF

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

STRM Relationship Type #2: INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

STRM Relationship Type #3: EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

STRM Relationship Type #4: SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

STRM Relationship Type #5: NO RELATIONSHIP

SCF control and Focal Document Element are unrelated; their content does not overlap.

Expert-Derived Content (EDC) vs Natural Language Processing (NLP)

NIST IR 8477 provides the "gold standard" practice for how an individual can perform crosswalk mapping with no technology needed, where it can literally be performed with a pencil and piece of paper. Children learn the process of diagramming sentences in grade school (e.g., Reed–Kellogg model) with pencils and paper. This is the process of graphically identifying nouns, verbs, adjectives and modifiers to teach proper sentence structure for how various components of language work together to communicate an idea. With the advent of Artificial Intelligence (AI), the ability to diagram sentences in both computer and human-readable format is achievable through Natural Language Processing (NLP).

From a cybersecurity crosswalking perspective, NLP can be used to evaluate a control statement (e.g., must have firewall) to identify the noun (e.g., firewall) and verb (e.g., must have) to determine the relative strength it maps to a different control (e.g., shall have network defense appliances). Where that becomes interesting is (1) protecting the underlying content (e.g., Intellectual Property (IP)) and (2) patentability.

Works created by non-humans, including AI, are not eligible for copyright protection.[16] While the SCF leverages expert-derived content (e.g., human subject-matter experts), other metaframework solutions use NLP to create AI-generated crosswalk mapping. Solutions leveraging NLP forfeit their IP since AI-generated content is currently prohibited from copyright protections due to the content not being the work of a human creator. Therefore, NLP-generated content could be considered free content from an IP perspective, since a copyright of AI-generated content would not be enforceable.

AI-based solutions in the GRC space also face a patentability issue due to the "mental steps" doctrine. In 2014, the US Supreme Court ruled that inventions are ineligible for patenting if the patent claim is something a human could do in their mind or with paper and pencil (e.g., a human performing sentence diagramming on a piece of paper and comparing the results of that sentence diagram with another). That landmark case (*Alice Corp. v. CLS Bank International*) established a new uncertainty about patent eligibility of AI and machine learning technologies. The result of Alice is that patents issued for compliance solutions leveraging NLP to perform crosswalk mapping may not hold up to scrutiny by the Patent Trial and Appeal Board (PTAB) given NIST published a document that describes how to perform crosswalk mapping without the assistance of technology.

[16] *37 CFR Part 202 - https://www.federalregister.gov/documents/2023/03/16/2023-05321/copyright-registration-guidance-works-containing-material-generated-by-artificial-intelligence*

Section 5. Understanding Fundamental Governance, Risk & Compliance (GRC) Functions

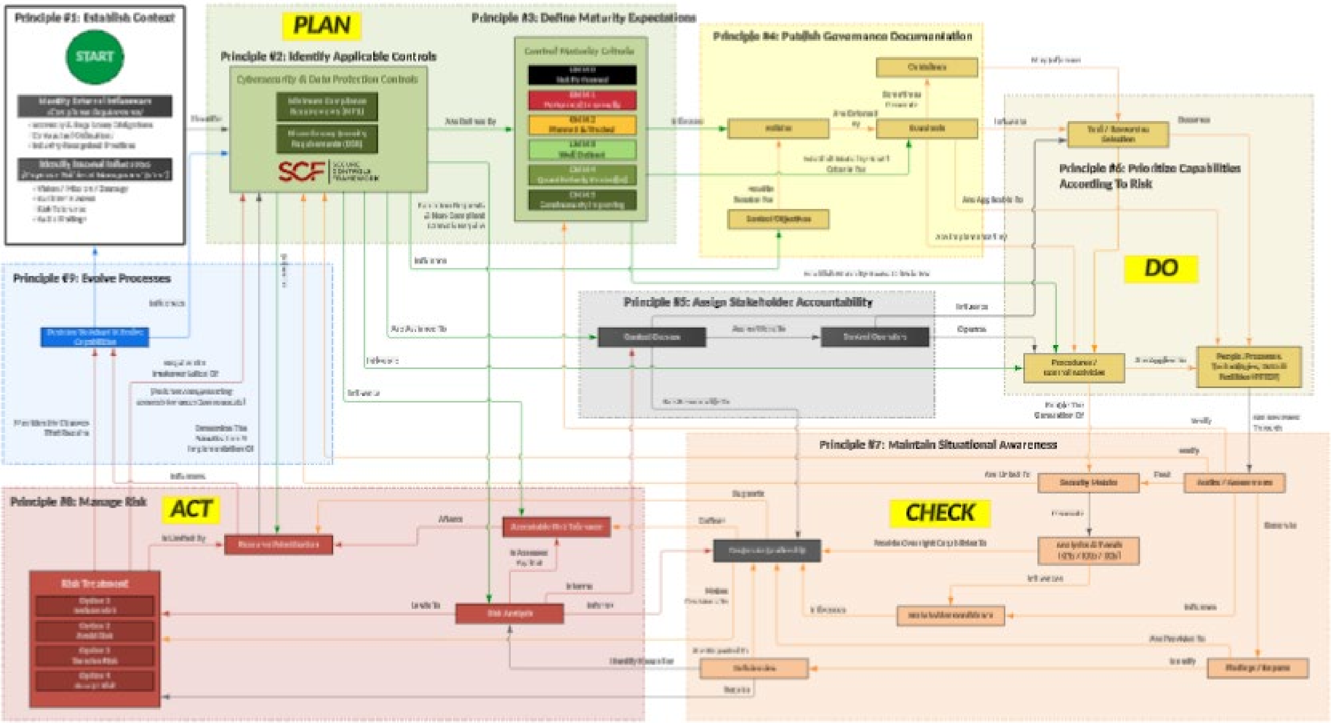
GRC can be a costly and labor-intensive endeavor, so what justifies the investment? Essentially, GRC functions help avoid negligence, with the added benefit of improved IT/cyber/privacy operating effectiveness. The reality of the situation is your company invests in cybersecurity & data privacy as a 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 & data privacy practices are ignored. Regardless of the specific reason, those charged with developing, implementing and running your organization's cybersecurity & data privacy 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, while help provide the ability to safely navigate 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 safely. 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.


Principle #1: Establish Context
START
PLAN
Principle #2: Identify Applicable Controls
Cybersecurity & Data Protection Controls
SCF
Principle #3: Define Maturity Expectations
Control Maturity Criteria
Principle #4: Publish Governance Documentation
Principle #6: Prioritize Capabilities According To Risk
DO
Principle #9: Evolve Processes
Principle #5: Assign Stakeholder Accountability
Principle #7: Maintain Situational Awareness
CHECK
Principle #8: Manage Risk
ACT
Risk Treatment

[graphic download - https://securecontrolsframework.com/content/Plan-Do-Check-Act.pdf]

Considering how business practices continuously evolve, so must cybersecurity practices. The Plan, Do, Check & Act (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 PPTDF 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 beings 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.

The premise is that controls are central to cybersecurity & data privacy operations as well as the business rhythms of the organization. Without properly defining MCR and DSR thresholds, an organization's overall cybersecurity & data 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., MCR vs. MCR+DSR) enhances risk management discussions.

Chicken vs Egg Debate: The Logical Order of GRC Functions

Which comes first? Governance, Risk or Compliance? This has been a hotly-debated topic since GRC was first coined nearly 20 years ago.[17] There is a logical order to GRC processes that must be understood to avoid siloes and an improperly scoped security program. First, it is necessary to level-set on the terminology of what GRC functions do:

- Governance. Structures the organization's controls to align with business goals and applicable statutory, regulatory, contractual and other obligations. Develops necessary policies and standards to ensure the proper implementation of controls.
- Risk Management. Identifies, quantifies and manages risk to information and technology assets, based on the organization's operating model.
- Compliance. Oversight of control implementation to ensure the organization's applicable statutory, regulatory, contractual and other obligations are adequately met. Conducts control validation testing and audits/assessments.

When establishing GRC practices, what is described below is the precedence of how (1) compliance influences (2) governance, which influences (3) risk management. This addresses the "GRC chicken vs egg" debate:

Compliance

The genesis of GRC is to first identify applicable statutory, regulatory and contractual obligations that the organization must adhere to, as well as internal business requirements (e.g., Board of Director directives). This is a compliance function that identifies statutory, regulatory and contractual obligations. It is a due diligence exercise to identify what the organization is reasonably required to comply with from a cybersecurity & data privacy perspective. This process involves interfacing with various Lines of Business (LOB) to understand how the organization operates, including geographic considerations. Generally, Compliance needs to work with the legal department, contracts management, physical security and other teams to gain a comprehensive understanding of the organizational compliance needs.

Compliance is the "source of truth" for statutory, regulatory and contractual obligations. With that knowledge, Compliance informs Governance about the controls that apply to applicable laws, regulations and frameworks. This knowledge is needed so that Governance can determine the appropriate policies and standards that must exist. Compliance may identify requirements to adhere to a specific industry framework (e.g., NIST CSF, ISO 27002, NIST 800-53, etc.), but organizations are usually able to pick the framework that best fits their needs on their own. This is often where various compliance obligations exceed what a single framework can address, so the organization must leverage some form of metaframework (e.g., framework of frameworks).

[17] *OCEG – What is GRC - https://www.oceg.org/ideas/what-is-grc/*

Compliance defines the controls necessary to meet the organization's specific needs (e.g., MCR + DSR) and publishes one or more control sets (e.g., specific to a project/contract/law/regulation or organization-wide controls). The control set(s) can be considered an organization's Minimum Security Requirements (MSR) that will be used:

- By the Governance team to develop appropriate policies, standards and other information (e.g., program-level guidance, Concept of Operations (CONOPS) documents, etc.; and
- By the Risk Management team to assess risk.

Given that not all controls are weighted equally, it is vitally important that personnel who represent the Risk Management function are involved in developing an assigned weight for each control (e.g., the presence of a fully-patched border firewall should be considered a more important control than end user awareness posters). This weighting of cybersecurity & data privacy controls is necessary to ensure the results of risk assessments accurate support the intent of the organization's risk tolerance threshold. That threshold is meant to establish a benchmark for defining acceptable and unacceptable risk.

GOVERNANCE

Based on these controls, Governance has two (2) key functions:

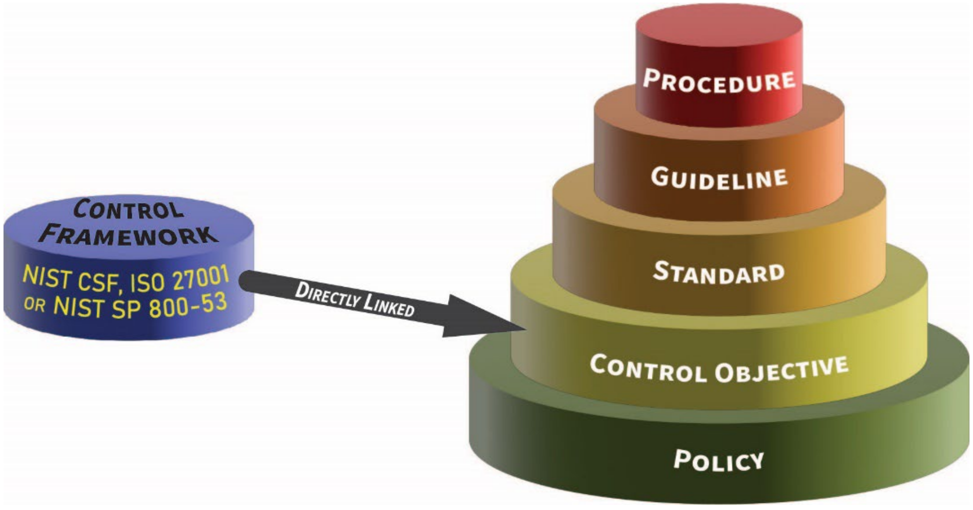
1. Develop policies and standards to meet those compliance obligations (defined by applicable control objectives); and
2. Assign ownership of those controls to the applicable stakeholders involved in the affected business processes. This process often requires a documented Responsibility, Accountability, Supportive, Consulted and Informed **(**RASCI**)** chart to ensure the organizational model supports effective implementation and oversight of the assigned controls.

Personnel representing the Governance function must work directly with the stakeholders (e.g., control owners and control operators) who are directly responsible for implementing and operating their assigned cybersecurity & data privacy controls. Those stakeholders are expected to develop and operate Standardized Operating Procedures (SOP) to ensure control implementation is performed according to the company's performance requirements, as established in the organization's cybersecurity & data privacy standards. The operation of those SOPs generates evidence of due care that reasonable practices are in place and operating accordingly. Generating deliverables is an expected output from executing procedures.

The development and implementation of the policies and standards is evidence of due diligence that the organization's compliance obligations are designed to address applicable administrative, technical and physical security controls. It is important to ensure that policies and standards document what the organization is doing, as the policies and standards are often the mechanisms by which outside regulators measure implementation and maturity of the control. Organizational governance can be a vital element in the organization's ability to implement, sustain and defend their compliance program.

Cybersecurity & data privacy documentation is generally comprised of six (6) main parts:

1. Policies establish management's intent;
2. Control Objectives identifies leading practices;
3. Standards provide quantifiable requirements;
4. Controls identify desired conditions that are expected to be met;
5. Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
6. Guidelines are recommended, but not mandatory.



This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

Risk Management

From a trickle-down perspective, while Risk Management logically follows both Compliance and Governance functions in establishing a GRC program, Risk Management is crucial for the organization to maintain situational awareness and remain both secure and compliant. Risk Management serves as the primary "canary in the coal mine" to identify instances of non-compliance that lead to the improper management of risks and exposure of the organization to threats; since ongoing risk assessments generally occur more frequently than internal/external audits that Compliance may oversee.

Risk Management activities addresses both due diligence and due care obligations to identify, assess and remediate control deficiencies:

- Risk Management must align with Governance practices for exception management (e.g., compensating controls).
- Compliance must evaluate findings from risk assessments and audits/assessments (both internal and external) to determine if adjustments to the organization's cybersecurity & data privacy controls (e.g., MCR + DSR) are necessary, based on business process changes, technology advancements and/or an evolution of the organization's risk threshold.

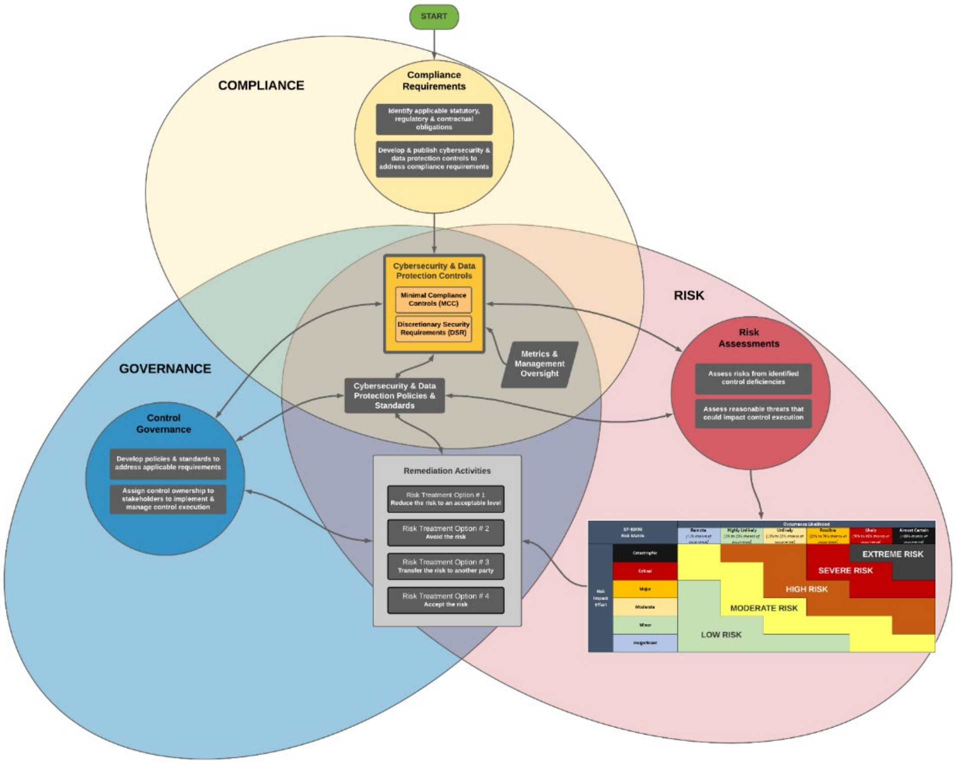
While Risk Management personnel do not perform the actual remediation actions (that is the responsibility of the control owner), Risk Management assists in determining the appropriate risk treatment options:

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

One key consideration for GRC, especially Risk Management, is that the appropriate level of organizational management makes the risk management decision. Therefore, risks need to be ranked, so that the appropriate levels of management can be designated as "approved authorities" to make a risk treatment determination. For example, a project manager should not be able to accept a "high risk" that should be made by a VP or some other executive. By formally assigning risk to individuals and requiring those in managerial roles to own their risk management decisions, it can help the organization maintain its target risk threshold.

GRC Integrations

The processes described above can be visualized in the following diagram which shows the interrelated nature of governance, risk management and compliance functions to build and maintain an organization's cybersecurity & data privacy program.


START
COMPLIANCE
Compliance Requirements
Identify applicable statutory, regulatory & contractual obligations
Develop & publish cybersecurity & data protection controls to address compliance requirements
Cybersecurity & Data Protection Controls
Minimal Compliance Controls (MCC)
Discretionary Security Requirements (DSR)
Metrics & Management Oversight
Cybersecurity & Data Protection Policies & Standards
RISK
Risk Assessments
Assess risks from identified control deficiencies
Assess reasonable threats that could impact control execution
GOVERNANCE
Control Governance
Develop policies & standards to address applicable requirements
Assign control ownership to stakeholders to implement & manage control execution
Remediation Activities
Risk Treatment Option # 1
Reduce the risk to an acceptable level
Risk Treatment Option # 2
Avoid the risk
Risk Treatment Option # 3
Transfer the risk to another party
Risk Treatment Option # 4
Accept the risk
SP-RMM
Risk Matrix
Occurrence Likelihood
Remote
Highly Unlikely
Unlikely
Possible
Likely
Almost Certain
Risk Impact Effect
Catastrophic
Critical
Major
Moderate
Minor
Insignificant
EXTREME RISK
SEVERE RISK
HIGH RISK
MODERATE RISK
LOW RISK

[graphic download - https://securecontrolsframework.com/content/GRC-Fundamentals.pdf]

SECTION 6. UNDERSTANDING WHAT IT MEANS TO ADOPT "SECURE BY DESIGN" PRINCIPLES

For an organization claims it "*just does ISO 27002*" it is easy to say, "*We're an ISO shop and we exclusively use ISO 27002 cybersecurity principles*" and that would be routinely accepted as being adequate. However, what about companies that have complex cybersecurity and compliance needs, such as a company that must address SOC2, ISO 27002, CCPA, EU GDPR, PCI DSS and NY DFS? In these complex cases that involve multiple frameworks, the reality is that ISO 27002 controls alone do not provide appropriate coverage. 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 cybersecurity & data protection processes but lack the knowledge and experience to undertake such documentation efforts. That means organizations are faced with either outsourcing 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 for requiring organizations to demonstrate cybersecurity & data privacy principles are by both "by default and by design," Secure Engineering & Data Privacy (SEDP) principles are not just limited to EU GDPR. SEDP principles are actually common requirements in the constantly-evolving statutory and regulatory landscapes. The following are common statutory, regulatory and contractual requirements that expect SEDP practices:

- AICPA Trust Services Principles (ESP) (e.g., System and Organization Controls (SOC) 2 Type 1) – CC2.2, CC3.2, CC5.1 & CC5.2
- Cloud Computing Compliance Controls Catalogue (C5) – KOS-01 & KOS-07
- Criminal Justice Information Services (CJIS) Security Policy – 5.10.1.1 & 5.10.1.5
- COBIT 2019 – DSS06.06
- COSO 2017 – Principles 10 & 11
- European Union Agency for Network and Information Security (ENISA) Technical Guideline of Security Measures – SO12
- European Union General Data Protection Regulation (EU GDPR) – Art 5.2, 24.1, 24.2, 24.3, 25.1, 25.2, 25.3, 32.1, 32.2 & 40.2
- Federal Risk and Authorization Management Program (FedRAMP) – SA-8, SC-7(18) & SI-01
- Food & Drug Administration (FDA) 21 CFR Part 11 – §11.30
- Federal Trade Commission (FTC) Act - §45(a) & §45b(d)(1)
- Generally Accepted Privacy Principles (GAPP) – 4.2.3, 6.2.2, 7.2.2 & 7.2.3
- Health Insurance Portability and Accountability Act (HIPAA) - 164.306, 164.308, 164.312, 164.314 & 164.530
- ISO 27002:2013 – 8.3.2
- ISO 27018 – A.10.1, A.10.4, A.10.5 & A.10.6
- ISO 29100 – 5.10 & 5.11
- National Industry Security Program Operating Manual (NISPOM) – 8-101, 8-302 & 8-311
- NIST SP 800-53 – PT-1, SA-8, SA-13, SC-7(18) & SI-1
- NIST SP 800-171 – 3.13.1, 3.13.3 & Non-Federal Organization (NFO)
- NIST Cybersecurity Framework – PR.IP-1
- Payment Card Industry Data Security Standard (PCI DSS) – 1.2, 1.3, 1.4, 1.5, 2.2, 6.5 & 12.5

COMPLIANCE SHOULD BE VIEWED AS 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 will often be a natural byproduct of those secure practices.

The SCF's comprehensive listing of over 1,200 cybersecurity & data protection controls is categorized into thirty-three (33) domains that are mapped to over 200 authoritative sources (e.g., statutory, regulatory and contractual frameworks). Those applicable SCF controls can operationalize the cybersecurity & data privacy principles to help an organization ensure that secure practices are implemented by design and by default.

You may be asking yourself, *"What cybersecurity & data privacy principles should I be using?"* and that is a great question. The SCF helped with this common question by taking the thirty-three (33) 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.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

Secure, Compliant & Resilient (SCR) Principles

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

The SCR is a set of thirty-three (33) cybersecurity & data privacy principles that leverage the SCF's extensive cybersecurity & data privacy control set. You can download the free poster at https://securecontrolsframework.com/domains-principles/.

Security & Privacy by Design Principles (S|P)

SCF | SECURE CONTROLS FRAMEWORK

1. Security & Privacy Governance
2. Asset Management
3. Business Continuity & Disaster Recovery
4. Capacity & Performance Planning
5. Change Management
6. Cloud Security
7. Compliance
8. Configuration Management
9. Continuous Monitoring
10. Cryptographic Protections
11. Data Classification & Handling
12. Embedded Technology
13. Endpoint Security
14. Human Resources Security
15. Identification & Authentication
16. Incident Response
17. Assurance
18. Maintenance
19. Mobile Device Management
20. Network Security
21. Physical & Environmental Security
22. Privacy
23. Project & Resource Management
24. Risk Management
25. Secure Engineering & Architecture
26. Security Operations
27. Security Awareness & Training
28. Technology Development & Acquisition
29. Third-Party Management
30. Threat Management
31. Vulnerability & Patch Management
32. Web Security

The "C 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.

Steps To Operationalize The SCR Principles

1. Read through the SCR principles to familiarize yourself with the thirty-three (33) domains to understand how they come together to address the cybersecurity, privacy and physical security considerations for a modern security program.
2. Identify the applicable SCF controls that your organization needs to implement to address its applicable statutory, regulatory and contractual compliance needs.
3. Implement and monitor those SCF controls to ensure the SCR principles are being met by your day-to-day practices.

The SCR establishes thirty-three (33) common-sense principles to guide the development and oversight of a modern cybersecurity & data privacy program. Those thirty-three (33) SCR principles are listed below:

SCF Domains & SCR Principles

#	SCF Domain	SCF Identifier	Secure, Compliant & Resilient (SCR) Principles	Principle Intent
1	Cybersecurity & Data Privacy Governance	GOV	Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses applicable statutory, regulatory and contractual obligations.	Organizations specify the development of an organization's cybersecurity & data protection program, including criteria to measure success, to ensure ongoing leadership engagement and risk management.
2	Artificial and Autonomous Technology	AAT	Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.	Organizations ensure Artificial Intelligence (AI) and autonomous technologies are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced. In addition, AI-related risks are governed according to technology-specific considerations to minimize emergent properties or unintended consequences.
3	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.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

4	Business Continuity & Disaster Recovery	BCD	Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.	Organizations establish processes that will help the organization recover from adverse situations with minimal impact to operations, as well as provide the capability for e-discovery.
5	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.
6	Change Management	CHG	Manage 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, including the assessment, authorization and monitoring of technical changes across the enterprise so as to not impact production systems uptime and allow easier troubleshooting of issues.
7	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 cybersecurity & data privacy 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.
8	Compliance	CPL	Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.	Organizations ensure controls are in place to ensure adherence to applicable statutory, regulatory and contractual compliance obligations, as well as internal company standards.
9	Configuration Management	CFG	Enforce secure configurations according to vendor-recommended and industry-recognized secure practices that enforce the concepts of “least privilege” and “least functionality” for all systems, applications and services.	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.
10	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.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

11	Cryptographic Protections	CRY	Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.	Organizations ensure the confidentiality and integrity of its data through implementing appropriate cryptographic technologies to protect systems, applications, services and data.
12	Data Classification & Handling	DCH	Enforce a standardized 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 electronic and physical, are properly classified and measures implemented to protect the organization's data from unauthorized disclosure, or modification, 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.
13	Embedded Technology	EMB	Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.	Organizations specify the development, proactive management and ongoing review of security embedded technologies, including hardening of the “stack” from the hardware, firmware and software to transmission and service protocols used for Internet of Things (IoT) and Operational Technology (OT) devices.
14	Endpoint Security	END	Harden endpoint devices to protect against reasonable threats to those devices and the data those devices 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.
15	Human Resources Security	HRS	Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.	Organizations create a cybersecurity & data privacy-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward and collaboration.
16	Identification & Authentication	IAC	Enforce the concept of “least privilege” consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.	Organizations implement the concept of “least privilege” through limiting access to the organization's systems and data to authorized users only.
17	Incident Response	IRO	Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).	Organizations establish and maintain a viable and tested capability to respond to cybersecurity or data privacy-related incidents in a timely manner, where organizational personnel understand how to detect and report potential incidents.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

18	Information Assurance	IAO	Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.	Organizations ensure the adequacy of cybersecurity & data privacy controls in development, testing and production environments.
19	Maintenance	MNT	Proactively 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.
20	Mobile Device Management	MDM	Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.	Organizations govern risks associated with mobile devices, regardless of ownership (organization-owned, employee-owned or third-party owned). Wherever possible, technologies are employed to centrally manage mobile device access and data storage practices.
21	Network Security	NET	Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of “least functionality” through restricting network access to systems, applications and services.	Organizations ensure sufficient cybersecurity & data 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.
22	Physical & Environmental Security	PES	Protect physical environments through 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.
23	Data Privacy	PRI	Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.	Organizations align data privacy engineering decisions with the organization's overall data privacy strategy and industry-recognized leading practices to secure Personal Data (PD) that implements the concept of data privacy by design and by default.
24	Project & Resource Management	PRM	Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.	Organizations ensure that security-related projects have both resource and project/program management support to ensure successful project execution.
25	Risk Management	RSK	Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk	Organizations ensure that the business unit(s) that own the assets and / or processes involved are made aware of and understand all applicable cybersecurity & data privacy-related

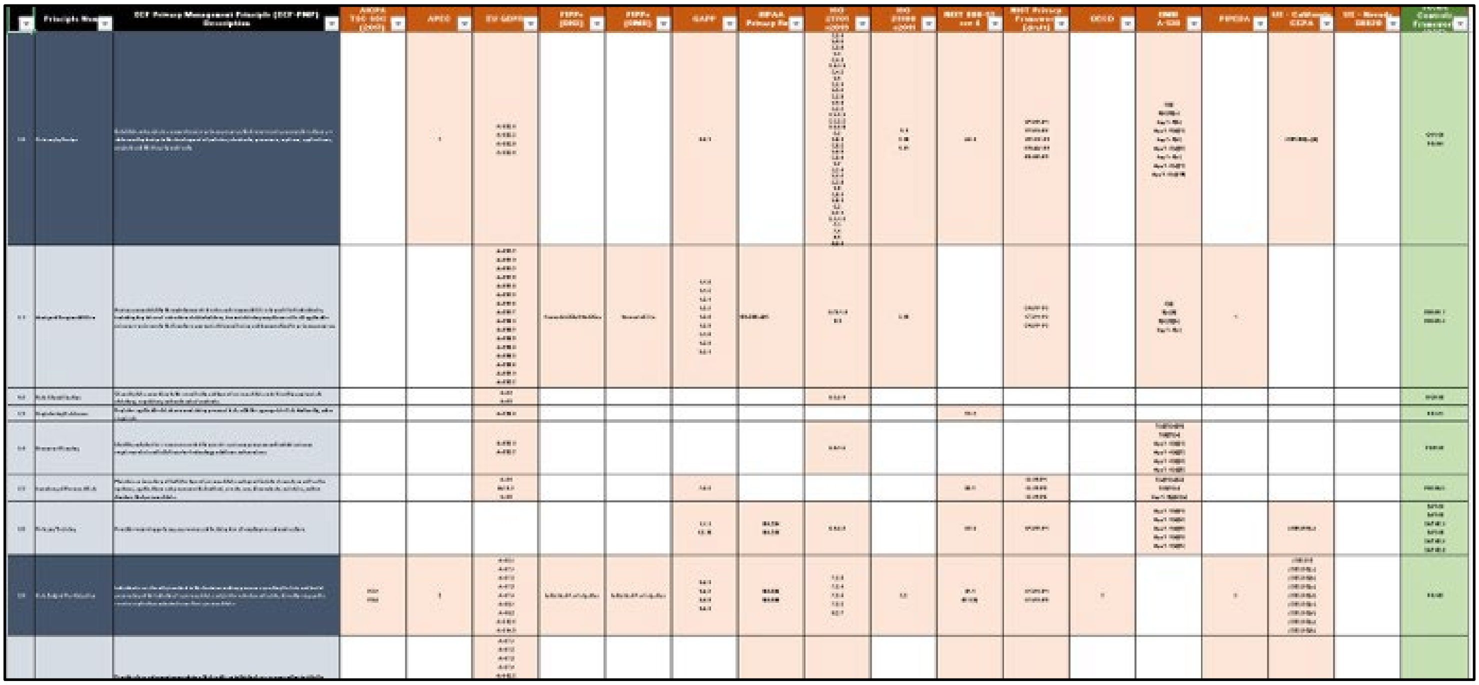
			decisions adhere to the organization's risk threshold.	risks. The cybersecurity & data privacy teams advise and educate on risk management matters, while it is the business units and other key stakeholders that ultimately own the risk.
26	Secure Engineering & Architecture	SEA	Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient 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.
27	Security Operations	OPS	Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.	Organizations ensure appropriate resources and a management structure exists to enable the service delivery of cybersecurity, physical security and data privacy operations.
28	Security Awareness & Training	SAT	Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.	Organizations develop a cybersecurity & data privacy-minded workforce through continuous education activities and practical exercises.
29	Technology Development & Acquisition	TDA	Develop and/or acquire systems, applications and services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design flaws.	Organizations ensure that cybersecurity & data privacy principles are implemented into any products/solutions, either developed internally or acquired, to make sure that the concepts of “least privilege” and “least functionality” are incorporated.
30	Third-Party Management	TPM	Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.	Organizations ensure that Secure, Compliant & Resilient Risks associated with third-parties are minimized and enable measures to sustain operations should a third-party become compromised, untrustworthy or defunct.
31	Threat Management	THR	Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.	Organizations establish a capability to proactively identify and manage technology-related threats to the cybersecurity & data privacy of the organization's systems, data and business processes.
32	Vulnerability & Patch Management	VPM	Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.	Organizations proactively manage the risks associated with technical vulnerability management that includes ensuring good patch and change management practices are utilized.
33	Web Security	WEB	Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring 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.

Section 7. Understanding What It Means To Adopt "Privacy by Design" 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 are built into the SCF, so you can leverage the SCF for both your cybersecurity & data privacy needs!

Why should you care? When you tie the broader SCR in with the SCF Data Privacy Management Principles (DPMP), you have an excellent foundation for building and maintaining secure systems, applications and services that address cybersecurity & data privacy considerations by default and by design. The DPMP is included in the SCF download as a separate tab in the Excel spreadsheet.[18]

Think of the SCF Privacy Management Principles as a supplement to the SCR 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 & data privacy control set, since we found the "apples to oranges" comparison between disparate privacy frameworks was difficult for most non-privacy practitioners to comprehend.



SCF Data Privacy Management Principles (DPMP)

For organizations, we found the "apples to oranges" comparison between disparate privacy frameworks was difficult for most non-privacy lawyers to understand. What this project did was identify a dozen of the leading privacy frameworks and create a set of simplified, yet comprehensive, privacy management principles. Below are the seventeen (17) different frameworks the SCF Data Privacy Management Principles are mapped to:

1. AICPA's Trust Services Criteria (TSC) SOC 2 (2017);
2. Asia-Pacific Economic Cooperation (APEC);
3. California Privacy Rights Act (CPRA);
4. European Union General Data Protection Regulation (EU GDPR);
5. Fair Information Practice Principles (FIPPs) - Department of Homeland Security (DHS);
6. Fair Information Practice Principles (FIPPs) - Office of Management and Budget (OMB);
7. Generally Accepted Privacy Principles (GAPP);
8. HIPAA Privacy Rule;
9. ISO 27701;
10. ISO 29100;
11. Nevada SB820;

[18] *SCF DPMP - https://securecontrolsframework.com/data-privacy-management-principles/*

12. NIST SP 800-53 R4;
13. NIST SP 800-53 R5;
14. NIST Privacy Framework v1.0;
15. Organization for Economic Co-operation and Development (OECD);
16. Office of Management and Budget (OMB) - Circular A-130; and
17. Personal Information Protection and Electronic Documents Act (PIPEDA).

We took these frameworks and looked for similarities and gaps. If you download the SCF Data Privacy Management Principles, you will see the direct mappings to these leading privacy frameworks. Given this, you now know the origin of the principle we include in our document. This is a great tool for organizations that may have to address multiple requirements because it brings a common language to simply things.

The eighty-six (86) principles of the SCF Data Privacy Management Principles 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; and
11. Business Environment.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

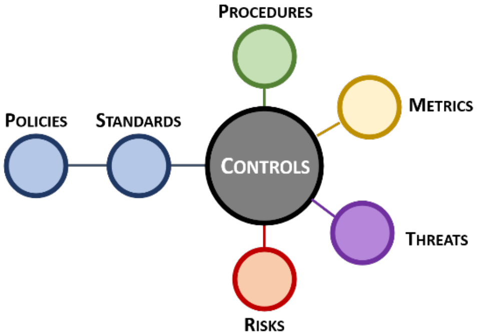
Section 8. Secure, Compliant & Resilient Management System (SCRMS)

The premise of Secure, Compliant & Resilient Management System (SCRMS) is that controls are central to cybersecurity & data privacy operations, as well as the overall business rhythm of an organization. This premise of the SCRMS is supported by the Secure, Compliant & Resilient Risk Management Model (SCR-RMM),[19] that describes the central nature of controls, where not just policies and standards map to controls, but procedures, metrics, threats and risks, as well.

SCRMS is defined as, *"a holistic, technology-agnostic approach to cybersecurity & data privacy controls to identify, implement and manage secure and compliant practices, covering an organization's people, processes, technology and data, regardless of how or where data is stored, processed and/or transmitted."*

SCRMS takes a different approach from the traditional definition of Governance, Risk Management and Compliance (GRC) and/or Integrated Risk Management (IRM), since SCRMS is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization's cybersecurity & data privacy operations.

SCRMS is designed to proactively address the strategic, operational and tactical nature of operating an organization's cybersecurity & data privacy program at the control level. SCRMS is designed to address both internal controls, as well as the broader concept of Supply Chain Risk Management (SCRM).



OCEG defines GRC as, "*GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity,*" while Gartner jointly defines GRC/IRM as, "*a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.*"

Secure and compliant operations exist when applicable controls are properly scoped and implemented. SCRMS 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, an organization's applicable controls are categorized according to "must have" vs "nice to have" requirements:

- Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- Discretionary Security Requirements (DSR) are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity & data privacy controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments. DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establishes the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

IT General Controls (ITGC)

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

Security vs Compliance

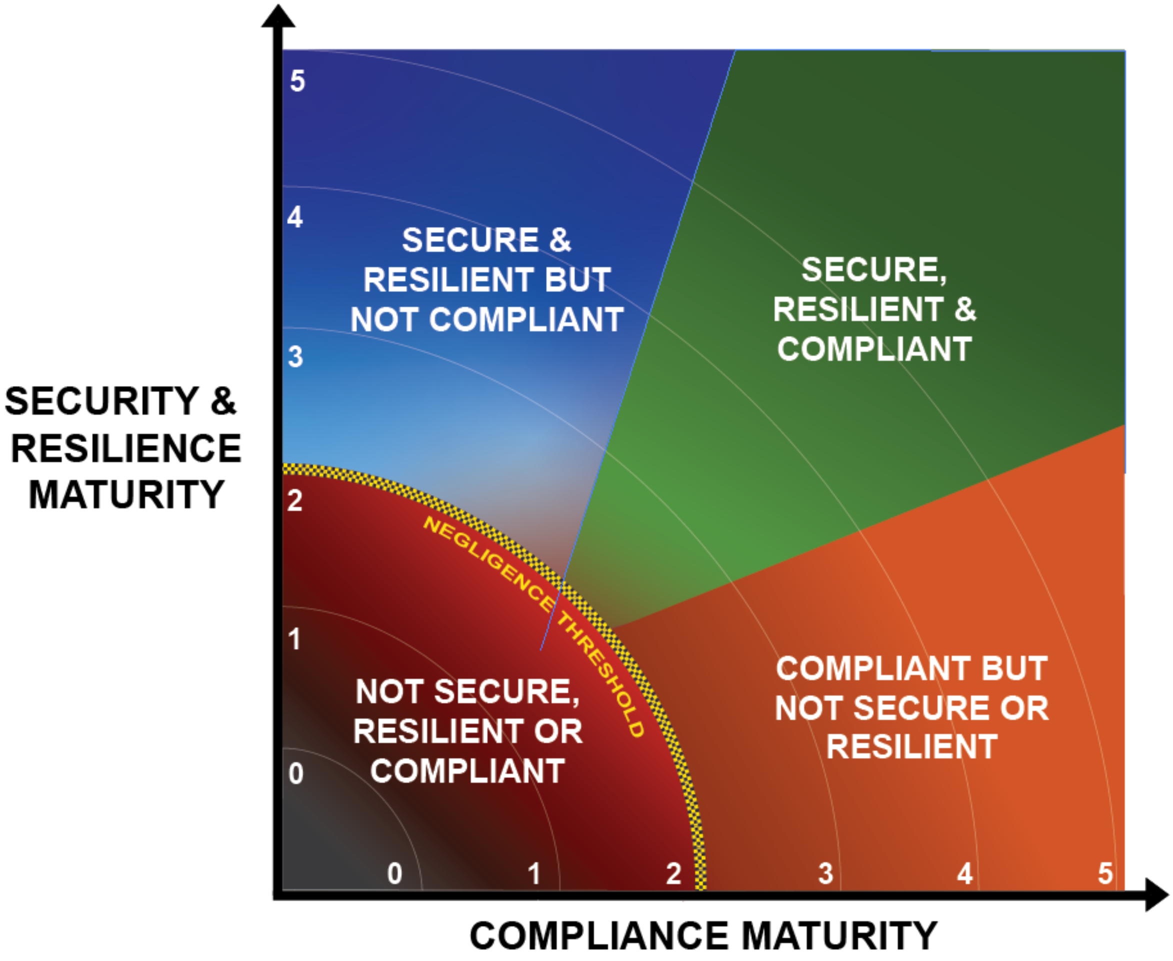
For those on the receiving end of cybersecurity efforts, the terms "security" and "compliance" might seem synonymous. However, understanding the subtle, yet crucial, differences between being compliant and being secure is paramount in safeguarding an organization's technologies and sensitive/regulated data.

[19] *SCF C|P-RMM - https://securecontrolsframework.com/risk-management-model/*

There is a long-running debate pertaining to "compliance is not security" and there is some truth to that saying. However, instead of a binary state of being singularly compliant or secure, it should be viewed as four (4) maturity-based quadrants where your organization is either:

1. Not secure, resilient or compliant (negligent);
2. Secure & resilient, but not compliant;
3. Compliant, but not secure or resilient; or
4. Secure, resilient & compliant.

The underlying issue in the "compliance vs security" debate is complacency and this is important for the broader concept of SCRMS. Your adversaries are unrelenting, so why would you consciously choose to settle? That is where the concept of negligence comes into play, when your failure to conduct due diligence and due care activities can be considered negligent behavior. That term tends to scare executives, and it should, but it does not change the reality that there is a negligence threshold that is specific to each organization. The question for you is, *"Do you know what your negligence threshold is, based on your applicable laws, regulations and contractual obligations?"*


SECURITY & RESILIENCE MATURITY
COMPLIANCE MATURITY
0
1
2
3
4
5
SECURE & RESILIENT BUT NOT COMPLIANT
SECURE, RESILIENT & COMPLIANT
NOT SECURE, RESILIENT OR COMPLIANT
COMPLIANT BUT NOT SECURE OR RESILIENT
NEGLIGENCE THRESHOLD

This concept of identifying a negligence threshold is addressed in the SCF's Secure, Compliant & Resilient Capability Maturity Model (SCR-CMM).[20]

MUST HAVE CONTROLS - DEFINING "BEING COMPLIANT" THAT IS SPECIFIC TO YOUR BUSINESS PROCESSES

Compliance controls are viewed as "must have" requirements that are non-discretionary (e.g., not optional). These requirements directly sourced from an organization's applicable laws, regulations and contractual obligations. The process of clearly identifying non-discretionary controls generally involves interviewing multiple stakeholders to gain appropriate situational awareness of all pertinent compliance obligations. These stakeholders with valuable insights are often:

- Process owners;
- Procurement / Contracts Management;
- Project Management Office (PMO);

[20] *SCF C|P-CMM - https://securecontrolsframework.com/capability-maturity-model/*

- Enterprise Risk Management (ERM);
- Legal;
- Physical Security; and
- Human Resources.

EXPERT INSIGHT (SCOPING): From a scoping perspective, compliance obligations may be organization-wide or narrowly scoped to a specific enclave or project. It is solely your organization's responsibility to properly scope the applicability of its applicable compliance controls. The Unified Scoping Guide (USG) is an excellent resource for your scoping exercise.[21]

NICE TO HAVE CONTROLS - DEFINING "SECURE & RELIANT" THAT IS SPECIFIC TO YOUR BUSINESS PROCESSES

Cybersecurity and data protection controls that are not required by a law, regulation or contractual obligation are "nice to have" controls that are discretionary for an organization to implement. Any aspect of non-compliance with a discretionary control would be isolated within the realm of the stakeholder making the requirement, since the requirement is internal to your organization. The source of these discretionary requirements may be from:

- Board of Director (BoD) guidance;
- Steering Committee recommendations;
- Internal Audit findings;
- Third-party audit/assessment recommendations; and/or
- Internal staff preferences.

The importance of these discretionary controls is that those are often organization-specific considerations to mitigate risk that is specific to an organization's business practices.

DISCRETIONARY CYBERSECURITY & DATA PROTECTION CONSIDERATIONS

A common frustration amongst cybersecurity practitioners is about the gaps that exist in many "best practice" cybersecurity frameworks. This is often where there are complaints about organizations holding an ISO 27001 certification, SOC 2 audit or PCI DSS audit that still have breaches or security incidents, where the argument is that a certification does not mean the organization is secure. The remedy to such gaps is through discretionary cybersecurity & data protection controls that are not directly mandated by a compliance obligation, such as the requirements for:

- Data Loss Prevention (DLP);
- Network Access Control (NAC);
- File Integrity Monitoring (FIM);
- 24/7 Security Operations Center (SOC);
- Artificial Intelligence (AI) governance controls;
- Sandboxing / detonation chambers;
- Segmented Dev / Test / Production environments;
- Cloud infrastructure-specific controls; and/or
- Embedded technology-specific controls.

DISCRETIONARY RESILIENCE CONSIDERATIONS

NIST defines resilience as, *"The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."*[22] From a discretionary control perspective, this may require the addition of technologies and processes to help ensure the continuity of business operations, such as:

- Continuity of Operations Plan (COOP);
- Business Continuity / Disaster Recovery (BC/DR) Plan;
- Failover / redundancy capabilities;
- Business continuity test exercises;
- Offsite, online backup storage;
- Offsite, offline backup storage; and/or
- Transactional-level backups.

[21] *Unified Scoping Guide - https://complianceforge.com/content/pdf/unified-scoping-guide-usg.pdf*

[22] *NIST Glossary - https://csrc.nist.gov/glossary/term/resilience#*

Defining Negligence As It Pertains To Cybersecurity & Data Privacy

The following content is leveraged from Cornell's Law School Legal Information Institute (LII)[23] to help provide some additional context to the previous points previously explained.

Negligent conduct may consist of either an act, or an omission to act when there is a duty to do so. Primary factors to consider in ascertaining whether the person's conduct lacks reasonable care are:

- The foreseeable likelihood that the person's conduct will result in harm;
- The foreseeable severity of any harm that may ensue; and
- The burden of precautions to eliminate or reduce the risk of harm.

Four (4) elements are generally required to establish a *prima facie* case of negligence:

1. Existence of a legal duty that the defendant owed to the plaintiff (*e.g., complying with NIST SP 800-171 to protect Controlled Unclassified Information (CUI)*);
2. Defendant's breach of that duty *(e.g., failure to protect CUI in accordance with NIST SP 800-171 requirements under applicable DFARS clauses*);
3. Plaintiff's sufferance of an injury (*e.g., financial losses due to lost contract due to non-compliance with NIST SP 800-171*); and
4. Proof that defendant's breach caused the injury (*e.g., publicity about the data breach or other evidence pointing to the entity being the source of the data breach*)

Typically, to meet the injury element of the *prima facie* case, the injury must be one (1) of two (2) things:

1. Bodily harm; or
2. Harm to property (can be personal property or business property (physical or digital)).

Determining A Breach Of Duty

When determining how whether the defendant has breached a duty, courts will usually use the *Learned Hand formula*[24], which is an algebraic approach to determining liability. If $B < PL$, then there will be negligence liability for the party with the burden of taking precautions where:

- B = Burden of taking precautions
- P = Probability of loss
- L = Gravity of loss

If the burden of taking such precautions is less than the probability of injury multiplied by the gravity of any resulting injury, then the party with the burden of taking precautions will have some amount of liability.

Determining Whether There Was A Duty To Act

Typically, if the defendant had a duty to act, did not act (resulting in a breach of duty) and that breach of duty caused an injury, then the defendant's actions will be classified as misfeasance. There are several ways to determine whether the defendant had a duty to act (this is not an exhaustive list):

- The defendant engaged in the creation of the risk which resulted in the plaintiff's harm;
- The defendant volunteered to protect the plaintiff from harm;
- The defendant knew / should have known that the conduct will harm the plaintiff; or
- Business/voluntary relationships.

SCRMS Principles

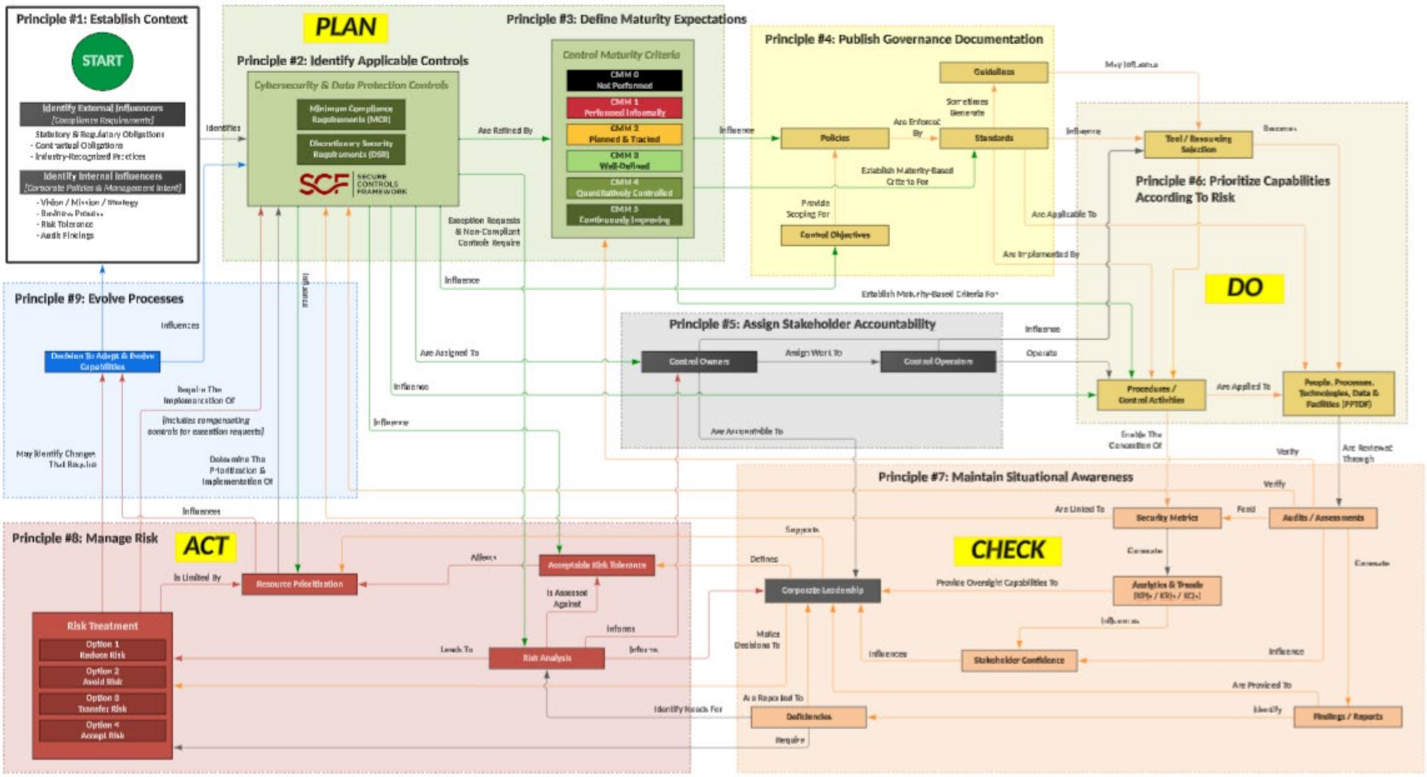
There are nine (9) principles associated with the Security, Compliance & Resilience Management System (SCRMS):

(1) Establish Context
(2) Identify Applicable Controls
(3) Define Maturity Expectations
(4) Publish Governance Documentation
(5) Assign Stakeholder Accountability
(6) Prioritize Capabilities According To Risk
(7) Maintain Situational Awareness
(8) Manage Risk

[23] *Cornell's Law School - https://www.law.cornell.edu/wex/negligence*
[24] *Learned Hand Formula - https://academic.oup.com/lpr/article/5/1/1/990799*

(9) Evolve Processes

NOTE: Principle #2 is where the Living Control Set (LCS) is established. As processes evolve and require adjustment, the LCS should be updated in Principle #9.



Principle #1: Establish Context
START
Identify External Influencers
[Compliance Requirements]
Statutory & Regulatory Obligations
- Contractual Obligations
- Industry-Recognized Practices
Identify Internal Influencers
[Corporate Policies & Management Intent]
- Vision / Mission / Strategy
- Business Practices
- Risk Tolerance
- Audit Findings
PLAN
Principle #2: Identify Applicable Controls
Cybersecurity & Data Protection Controls
Minimum Compliance Requirements (MCR)
Discretionary Security Requirements (DSR)
SCF SECURE CONTROLS FRAMEWORK
Identifies
Are Refined By
Principle #3: Define Maturity Expectations
Control Maturity Criteria
CMM 0 Not Performed
CMM 1 Performed Informally
CMM 2 Planned & Tracked
CMM 3 Well-Defined
CMM 4 Quantitatively Controlled
CMM 5 Continuously Improving
Exception Requests & Non-Compliant Controls Require
Influence
Principle #4: Publish Governance Documentation
Guidelines
Sometimes Generate
Policies
Are Enforced By
Standards
Establish Maturity-Based Criteria For
Provide Scoping For
Control Objectives
May Influence
Influence
Tool / Resourcing Selection
Becomes
Principle #6: Prioritize Capabilities According To Risk
Are Applicable To
Are Implemented By
DO
Establish Maturity-Based Criteria For
Principle #5: Assign Stakeholder Accountability
Control Owners
Assign Work To
Control Operators
Influence
Operate
Are Assigned To
Procedures / Control Activities
Are Applied To
People, Processes, Technologies, Data & Facilities (PPTDF)
Are Accountable To
Enable The Generation Of
Verify
Are Reviewed Through
Principle #9: Evolve Processes
Influences
Decision To Adapt & Evolve Capabilities
Require The Implementation Of
[Includes compensating controls for exception requests]
May Identify Changes That Require
Determine The Prioritization & Implementation Of
Influence
Influence
Influences
Principle #8: Manage Risk
ACT
Is Limited By
Resource Prioritization
Affects
Acceptable Risk Tolerance
Is Assessed Against
Informs
Leads To
Risk Analysis
Informs
Identify Needs For
Risk Treatment
Option 1 Reduce Risk
Option 2 Avoid Risk
Option 3 Transfer Risk
Option 4 Accept Risk
Principle #7: Maintain Situational Awareness
Verify
Are Linked To
Security Metrics
Feed
Audits / Assessments
Supports
Defines
CHECK
Generate
Generate
Corporate Leadership
Provide Oversight Capabilities To
Analytics & Trends (KPIs / KRIs / KCIs)
Influences
Makes Decisions To
Influences
Stakeholder Confidence
Influence
Are Provided To
Are Reported To
Deficiencies
Identify
Findings / Reports
Require

[graphic download - https://securecontrolsframework.com/content/plan-do-check-act.pdf]

SCRMS Principle 1: Establish Context

To build and maintain efficient and effective operations, a cybersecurity and data protection program must have a hierarchical vision, mission and strategy that directly supports the entity'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), internal directives (e.g., Board of Directors, corporate policies, etc.). This also includes understanding applicable risks and threats, since the entity's exposure to those may influence the need for controls beyond those that are mandated as compliance obligations.

Establishing context is both a due diligence and due care element of an entity's cybersecurity and data protection program, since context changes with time. Things to consider when establishing context:

- Mission / vision / strategy of the entity;
- Statutory (law), regulatory (regulation) and contractual requirements for cybersecurity and data protection;
- Fiscal constraints;
- The entity's structure;
- The entity's risk profile (including risk appetite, risk tolerance and risk threshold considerations);
- Planned organizational changes (e.g., Mergers, Acquisitions & Divestitures (MA&D));
- Corporate culture (e.g., how receptive is the entity to change); and
- Geographic-specific requirements.

SCF Council Guidance

Part of an entity's due diligence activities involve establishing the context for the SCRMS. Practical steps to establish context for the SCRMS include talking with representatives outside of IT and cybersecurity to document the following information:

(1) The entity's structure:

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

- a. *Reporting structure (e.g., chain of command);*
  - b. *IT / cybersecurity governance stakeholders;*
  - c. *Supply chain partners; and*
  - d. *Geographic locations;*
- (2) *The entity's:*
  - a. *Mission;*
  - b. *Vision; and*
  - c. *Strategy;*
- (3) *Risk management practices:*
  - a. *Risk tolerance;*
  - b. *Risk appetite; and*
  - c. *Risk thresholds; and*
- (4) *Constraints the affect business operations:*
  - a. *Applicable legal obligations:*
    - i. *Statutory (law);*
    - ii. *Regulatory (regulation); and*
    - iii. *Contractual requirements;*
  - b. *Fiscal constraints; and*
  - c. *Corporate culture (e.g., how receptive the entity is to change).*

SCRMS Principle 2: Identify Applicable Controls

A tailored set of cybersecurity and data protection controls must exist for an entity to implement a SCRMS. This control set needs to be tailored for the entity's unique requirements, such as a combination of Minimum Compliance Requirements (MCR) and Discretionary Security Requirements (DSR). This blend of "must have" and "nice to have" requirements establish an entity's tailored control set to help ensure secure, compliant and resilient capabilities.

<u>SCF Council Guidance</u>

Part of an entity's due diligence process is to identify applicable cybersecurity and data protection controls. Practical steps to identify applicable controls include:

- (1) *Reading through the Secure Controls Framework (SCF) principles to become familiar with the thirty-three (33) domains to understand how they come together to address the security, compliance and resilience considerations for a modern cybersecurity and data protection program.*
- (2) *As "business enablers," CISOs should talk with representatives outside of IT and cybersecurity to gain an understanding of the entity's complete scope of compliance requirements (e.g., legal, procurement, physical security, etc.).*
- (3) *Developing a list of the "must have" laws, regulations and frameworks that the entity must comply with.*
- (4) *Developing a list of "nice to have" requirements that the entity's Board of Directors, or other stakeholders, feel are necessary.*

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

There is no expectation for an entity to utilize all 1,400+ controls in the SCF catalog. It is best to visualize the SCF as a "buffet of cybersecurity and data protection controls," where the entity only selects those controls necessary to address its unique requirements. Once the entity knows what is applicable, it is possible to use the SCF to generate a customized control set that is specific to address the entity's MCR and DSR.

Things to consider when defining applicable controls:

- ▪ *Controls to address "must have" requirements from laws, regulations and contractual obligations to ensure the entity is compliant with its obligations;*
- ▪ *Controls to address "discretionary" requirements that exist to ensure the entity has secure and resilient operations; and*

- *There needs to be at least an annual review to ensure the applicable controls are accurate to the current needs for compliance, security and resilience.*

SCRMS Principle 3: Define Maturity Expectations

The entity must define maturity expectations for its cybersecurity and data protection controls. From the perspective of the SCRMS, the maturity expectations define entity-specific "what right looks like" expectations for control implementation and continued operation. The maturity-based criteria are applicable to People, Processes, Technologies, Data & Facilities (PPTDF).

Maturity targets are expected to directly support the entity's need for security, compliance and resiliency capabilities. These maturity targets can be used by an entity's leadership for:

(1) Multi-year business planning;
(2) Budgeting; and
(3) Assessment criteria.

SCF Council Guidance

The SCF uses the Security, Compliance & Resilience Capability Maturity Model (SCR-CMM) criteria for each control. The SCR-CMM is an available option for maturity expectations for entities that lack maturity targets.

The SCR-CMM draws upon the high-level structure of the Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM), where it can be used to demonstrate varying levels of maturity for PPTDF at a control level.

Things to consider when assigning maturity-based criteria:

- *Not all controls need to be the same level of maturity, since each control has an associated cost. The higher the level of maturity, the higher the cost. This is a risk management decision to define what right looks like for the entity;*
- *The expected level of maturity needs to at least comply with applicable statutory, regulatory and contractual requirements; and*
- *Lower levels of maturity may be considered negligent behavior from a due care perspective.*

SCRMS Principle 4: Publish Governance Documentation

Cybersecurity and data protection documentation must exist, otherwise an entity's governance practices are both unenforceable and indefensible. Formalizing entity-specific requirements via documented policies, standards and procedures are necessary to operationalize cybersecurity and data protection controls.

Documented policies, standards and procedures provide evidence of due diligence that the entity identified and implemented reasonable steps to address its applicable requirements. The output of procedures provides evidence of due care that controls were operated as described.

SCF Council Guidance

There are generally three (3) options to generate cybersecurity and data protection 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.

Things to consider when publishing policies & standards:

- *Departments other than cybersecurity and data privacy publish policies, standards and procedures (e.g., HR, IT, Procurement, Legal, etc.) and those need to be reconciled to ensure interoperability.*
- *The policies and standards need to reflect both the "must have" and "nice to have" requirements identified in SCRMS Principle 2;*
- *Policies are designed as "high level statements of management intent" and are not expected to change often;*

- *Standards should be designed to assign granular requirements to enforce policies. As technologies change/evolve, those standards must be reviewed and updated, as necessary, to ensure secure, compliant and resilient capabilities; and*
- *Procedures should be written at a level of detail that makes it repeatable through clear steps, but should avoid unnecessary content that makes the procedures too difficult to maintain. As business processes or technologies change, procedures must be updated to reflect the new method(s) necessary to operate a control.*

SCRMS 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" are expected to 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.

SCF Council Guidance

Assigning stakeholder accountability offers unique challenges for entities, since it is beyond IT, cybersecurity and data protection. Common stakeholders involve 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 requires inter-departmental enforcement by an entity's management.

Things to consider when assigning stakeholder accountability:

- *Procedures are not "owned" by the cybersecurity or privacy teams. Procedures are the responsibility of the control owner / operator; and*
- *The NIST SP 800-181, Workforce Framework for Cybersecurity (NICE Framework), is a methodology to identify cybersecurity and data protection-related roles and associated responsibilities. The NICE Framework offers an efficient way to assign stakeholder accountability for internal and external stakeholders.*

SCRMS Principle 6: Prioritize Capabilities According To Risk

Security, compliance and resilience capabilities must be prioritized based on applicable risks and threats. Not all risks and threats are equal, so a risk-based prioritization must occur.

SCF Council Guidance

Prioritization should be based on a CISO-level business plan that supports the entity's broader mission and strategy. That department-level business plan would reasonably be a multi-year approach to address security, compliance and resilience capabilities. That formalized plan is used for resource allocation (e.g., staffing, technology purchases, service contracts, etc.) based on approval from the entity's executive leadership.

Things to consider when prioritizing capabilities:

- *Resources are finite, so a prioritized plan is expected to be spread out across multiple years; and*
- *The entity's executive leadership is expected to approve the prioritized plan, where the decision for the approved Course of Action (CoA) is elevated above the CISO role.*

SCRMS Principle 7: 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 (e.g., analytics). When properly tied in with current audits, control deficiencies, risk, threat and vulnerability information, this broader insight provides “situational awareness” that is necessary for an entity’s leadership to adjust plans to operate within the defined risk threshold.

SCF Council Guidance

Things to consider when maintaining situation awareness:

- *Metrics/analytics tell the long-term story of how the cybersecurity and data protection program is doing. This historical performance provides context to an entity’s senior leaders for decision-making purposes; and*
- *The metrics/analytics need to be tied to measurable controls that can help eliminate Fear, Uncertainty and Doubt (FUD) reporting.*

Maintaining situational awareness has different meanings, based on the security culture of an entity. Metrics / analytics reporting is often plagued by the problem of Garbage In, Garbage Out (GIGO). Often, the GIGO issue is rooted in an entity’s executive leadership trying to explain their perceived needs for metrics to cybersecurity practitioners in a way that describes the design of a "football bat" (e.g., nonsensical solution). To combat GIGO, it is advisable to approach the problem from the perspective that executive management often just wants a simple answer to a relatively-straightforward question: “Are we secure?” The metrics and analytics should be able to answer that question with irrefutable evidence.

SCRMS Principle 8: Manage Risk

Proactive risk management processes must exist across all phases of Technology Assets, Applications, Services and/or Data (TAASD) life cycles to address Confidentiality, Integrity, Availability and Safety (CIAS) aspects. Based on finite resources (e.g., time, personnel and money), it is necessary to utilize prioritized risk management practices that ensure issues posing the highest risk are addressed first.

Risk management must address internal and external factors, including data privacy, Artificial Intelligence (AI), embedded technology and Supply Chain Risk Management (SCRM) considerations. To manage risk, it requires the entity to enforce a clearly-defined risk threshold and ensure reasonable security practices are operational.

SCF Council Guidance

Risk management involves coordinated activities that optimize the management of potential opportunities and adverse effects. Proactive risk management activities provide a way to realize potential opportunities without exposing an entity to unnecessary peril.

The goal of risk analysis is to determine the potential negative implications of an action or situation to determine one (1) of two (2) decisions:

(1) Acceptable Risk: the criteria fall within a range of acceptable parameters; or
(2) Unacceptable Risk: The criteria fall outside a range of acceptable parameters.

Traditional risk management practices have four (4) options to address identified risk:

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

In a mature risk program, the results of risk assessments are evaluated with the entity's risk appetite into consideration. For example, if the entity has a Moderate Risk Appetite and there are several findings in a risk assessment that are High Risk, then action must be taken to reduce the risk. Accepting a High Risk would violate the Moderate Risk Appetite set by management. In reality, this leaves remediation, transferring or avoiding as the remaining three (3) options, since accepting the risk would be prohibited.

There are many ways to manage risk. However, the SCF’s Security, Compliance & Resilience Secure, Compliant & Resilient Risk Management Model (SCR-RMM) contains a control-centric:

- *Risk catalog;*
- *Threat catalog; and*
- *Methodology to not only perform a risk assessment, but manage risk across the entity.*

The value of the SCR-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 SCR-RMM makes calculating risk a straightforward process.

Controls are the nexus of a cybersecurity and data protection program, so it is vitally important to understand how controls should be viewed from a high-level risk management perspective. To progress from identifying a necessary control to a determination of risk, it is a journey that has several steps, each with its own unique terminology. Therefore, it is important to baseline the understanding of risk management terminology.

SCRMS Principle 9: 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 (e.g., Deming Cycle) to ensure the entity 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.

Things to consider when evolving processes:

- Changes in the compliance landscape (e.g., laws, regulations and contractual obligations);
- Technology changes; and
- Budget/resourcing constraints that affect how processes are implemented.

SCF Council Guidance

Things to consider when evolving processes:

- *Changes in the compliance landscape (e.g., laws, regulations and contractual obligations);*
- *Technology changes; and*
- *Budget/resourcing constraints that affect how processes are implemented.*

Without an overarching concept of operations for the SCRMS, entities will often find that their governance, risk management, compliance and data 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 PPTDF.

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

*(1) **Plan**. The overall SCRMS process beings with planning. This planning will define the policies, standards and controls for the entity. It will also directly influence the tools and services that an entity purchases, since technology purchases should address needs that are defined by policies and standards.*

*(2) **Do**. Arguably, this is the most important section for cybersecurity and data protection practitioners. Controls are the “security glue” that make processes, applications, systems and services secure. Procedures (also referred to as control activities) are the processes in which the controls are actually implemented and performed.*

*(3) **Check**. In simple terms, this is situational awareness. Situational awareness is only achieved through reporting through metrics and reviewing the results of audits/assessments.*

*(4) **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 entity.*

SECTION 9. SECURE, COMPLIANT & RESILIENT CAPABILITY MATURITY MODEL (SCR-CMM)

The SCR-CMM is meant to solve the problem of objectivity in both establishing and evaluating cybersecurity and data privacy controls. There are four (4) main objectives for the SCR-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;
3. Provide minimum criteria that can be used to evaluate third-party service provider controls; and
4. Provide a means to perform due diligence of cybersecurity and data privacy practices as part of Mergers & Acquisitions (M&A).

There are likely many other use cases that the SCR-CMM can be used, but those 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 common frustrations that exist in most cybersecurity and data 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.

WELL ESTABLISHED MATURITY MODEL

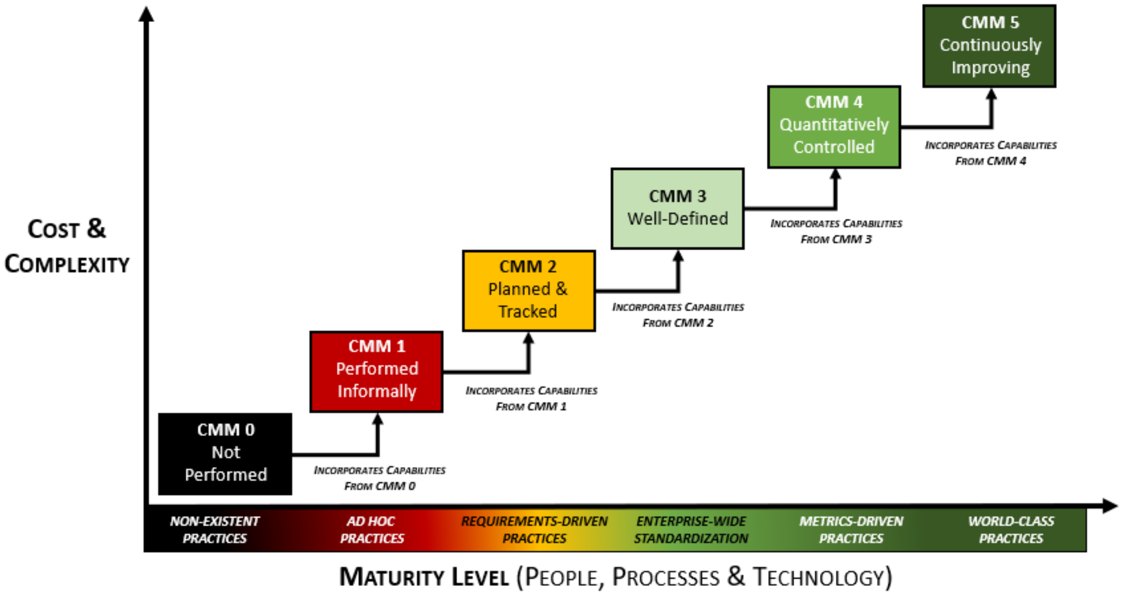
There are many competing models that exist to demonstrate maturity. Given the available choices, the SCF decided to leverage an existing framework, rather than reinvent the wheel. In simple terms, we provided control-level criteria to an existing CMM model.

The SCR-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 PPTDF 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).[25]

The SSE-CMM has been around for over two decades and is a community-owned maturity model, so it is free to use. The SSE-CMM is also referenced as ISO/IEC 21827:2008 *Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM).*[26]

NESTED APPROACH TO MATURITY

By using the term "nested" regarding maturity, we refer to how the SCR-CMM's control criteria were written to acknowledge that each succeeding level of maturity is built upon its predecessor. Essentially, you cannot run without first learning how to walk. Likewise, you cannot walk without first learning how to crawl. This approach to defining cybersecurity & privacy control maturity is how the SCR-CMM is structured.


Cost & Complexity
CMM 0 Not Performed
Incorporates Capabilities From CMM 0
CMM 1 Performed Informally
Incorporates Capabilities From CMM 1
CMM 2 Planned & Tracked
Incorporates Capabilities From CMM 2
CMM 3 Well-Defined
Incorporates Capabilities From CMM 3
CMM 4 Quantitatively Controlled
Incorporates Capabilities From CMM 4
CMM 5 Continuously Improving
Non-Existent Practices
Ad Hoc Practices
Requirements-Driven Practices
Enterprise-Wide Standardization
Metrics-Driven Practices
World-Class Practices
Maturity Level (People, Processes & Technology)

[25] Defense Technical Information Center (DTIC) - https://apps.dtic.mil/dtic/tr/fulltext/u2/a393329.pdf
[26] ISO/IEC 21827:2008 - https://www.iso.org/standard/44716.html

MATURITY (GOVERNANCE) ≠ ASSURANCE (SECURITY)

It is unfortunate that it must be explicitly stated, but a "maturity model" is entirely dependent upon the ethics and integrity of the individual(s) involved in the evaluation process. This issue is often rooted in the assessor's perceived pressure that a control should be designated as being more mature than it is (e.g., dysfunctional management influence). Regardless of the reason, it must be emphasized that consciously designating a higher level of maturity (based on objective criteria) to make an organization appear more mature should be considered fraud. Fraud is a broad term that includes *"false representations, dishonesty and deceit."*[27]

This stance on fraudulent misrepresentations may appear harsh, but it accurately describes the situation. There is no room in cybersecurity and data protection operations for unethical parties, so the SCF Council published this guidance on what a "reasonable party perspective" should be. This provides objectivity to minimize the ability of unethical parties to abuse the intended use of the SCR-CMM.

The following two (2) questions should be kept in mind when evaluating the maturity of a control (or Assessment Objective (AO)).

1. *Do I have reasonable evidence to defend my analysis/decision?*
2. *If there was an incident and I was deposed in a legal setting, can I justify my analysis/decision without perjuring myself?*

Do you need to answer "yes" to every bullet pointed criteria under a level of maturity in the SCR-CMM? No. We recognize that every organization is different. Therefore, the maturity criteria items associated with SCF controls are to help establish what would reasonably exist for each level of maturity. Fundamentally, the decision comes down to assessor experience, professional competence and common sense.

While a more mature implementation of controls can equate to an increased level of security, higher maturity and higher assurance are not mutually inclusive. From a practical perspective, maturity is simply a measure of governance activities pertaining to a specific control or set of controls. Maturity does not equate to an in-depth analysis of the strength and depth of the control being evaluated (e.g., rigor).

According to NIST, assurance is *"grounds for confidence that the set of intended security controls in an information system are effective in their application."*[28] Increased rigor in control testing is what leads to increased assurance. Therefore, increased rigor and increased assurance are mutually inclusive.

The SCF Conformity Assessment Program (SCF CAP) leverages (3) three levels of rigor. The SCF CAP's levels of rigor utilize maturity-based criteria to evaluate a control, since a maturity target can provide context for "what right looks like" at a particular organization:[29]

- **Level 1 (Basic)** - Basic assessments provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors.
- **Level 2 (Focused)** - Focused assessments provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious / apparent errors and whether there are increased grounds for confidence that the safeguards are implemented correctly and operating as intended.
- **Level 3 (Comprehensive)** - Comprehensive assessments provide a level of understanding of the security measures necessary for determining whether the safeguards are implemented and free of obvious errors and whether there are further increased grounds for confidence that the safeguards are implemented correctly and operating as intended on an ongoing and consistent basis and that there is support for continuous improvement in the effectiveness of the safeguards.

DEFINING SCR-CMM LEVELS

A summary of the six (6) SCR-CMM levels are described below:

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

[27] *US Department of Justice - https://www.justice.gov/archives/jm/criminal-resource-manual-1007-fraud*
[28] *US Department of Justice - https://www.justice.gov/archives/jm/criminal-resource-manual-1007-fraud*
[29] *SCF CAP - https://securecontrolsframework.com/scf-conformity-assessment-program-cap/*

SCR-CMM Level 0 (L0) - Not Performed

This level of maturity is defined as "non-existence practices," where the control is not being performed:

- Practices are non-existent, where a reasonable person would conclude the control is not being performed.
- Evidence of due care[30] and due diligence[31] do not exist to demonstrate compliance with applicable statutory, regulatory and/or contractual obligations.

L0 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 is 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 L0 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 scope in its support contract that excludes the control through either oversight or ignorance of the client's requirements.*
- *For medium / large organizations, there is IT and/or cybersecurity staff, but governance is functionally non-existent and the control is not performed through either oversight, ignorance or incompetence.*

SCR-CMM Level 1 (L1) - Performed Informally

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

- Practices are "ad hoc" where the intent of a control is not met due to a lack consistency and formality.
- When the control is met, it lacks consistency and formality (e.g., rudimentary practices are performed informally).
- A reasonable person would conclude the control is not consistently performed in a structured manner.
- Performance depends on specific knowledge and effort of the individual performing the task(s), where the performance of these practices is not proactively governed.
- Limited evidence of due care and due diligence exists, where it would be difficult to legitimately disprove a claim of negligence for how cybersecurity/privacy controls are implemented and maintained.

L1 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 L1 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 and/or cybersecurity staff but there is no management focus to spend time or resources on the control.*

SCR-CMM Level 2 (L2) - Planned & Tracked

Practices are "requirements-driven" where the intent of control is met in some circumstances, but not standardized across the entire organization:

- Practices are "requirements-driven" (e.g., specified by a law, regulation or contractual obligation) and are tailored to meet those specific compliance obligations (e.g., evidence of due diligence).
- Performance of a control is planned and tracked according to specified procedures and work products conform to specified standards (e.g., evidence of due care).
- Controls are implemented in some, but not all applicable circumstances/environments (e.g., specific enclaves, facilities or locations).
- A reasonable person would conclude controls are "compliance-focused" to meet a specific obligation, since the practices are applied at a local/regional level and are not standardized practices across the enterprise.
- Sufficient evidence of due care and due diligence exists to demonstrate compliance with specific statutory, regulatory and/or contractual obligations.

L2 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. L2 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, CMMC, NIST 800-171, etc.).

It can be argued that L2 practices focus more on compliance over security. The reason for this is the scoping of L2 practices are

[30] *Due care is the standard of care where a reasonable person would exercise in the same situation or under similar circumstances. This standard of care is used to determine whether a party's actions (or inactions) were negligent.*

[31] *Due diligence is the care that a reasonable person exercises to avoid harm to other persons or their property.*

narrowly-focused and are not enterprise-wide.

NOTE: The reality with a L2 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.*

SCR-CMM Level 3 (L3) - Well Defined

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

- Practices are standardized "enterprise-wide" where the control is well-defined and standardized across the entire enterprise.
- Controls are implemented in all applicable circumstances/environments (deviations are documented and justified).
- Practices are performed according to a well-defined process using approved, tailored versions of standardized processes.
- Performance of a control is according to specified well-defined and standardized procedures.
- Control execution is planned and managed using an enterprise-wide, standardized methodology.
- A reasonable person would conclude controls are "security-focused" that address both mandatory and discretionary requirements. Compliance could reasonably be viewed as a "natural byproduct" of secure practices.
- Sufficient evidence of due care and due diligence exists to demonstrate compliance with specific statutory, regulatory and/or contractual obligations.
- The Chief Information Security Officer (CISO), or similar function, develops a security-focused Concept of Operations (CONOPS) that documents organization-wide management, operational and technical measures to apply defense-in-depth techniques (in this context, a CONOPS is a verbal or graphic statement of intent and assumptions regarding operationalizing the identified tasks to achieve the CISO's stated objectives. The result of the CONOPS is operating the organization's cybersecurity and data protection program so that it meets business objectives). Control or domain-specific CONOPS may be incorporated as part of a broader operational plan for the cybersecurity and data privacy program (e.g., cybersecurity-specific business plan).

L3 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 L2 practices that are narrowly focused, L3 practices are standardized across the organization.

It can be argued that L3 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 L3 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.*

SCR-CMM Level 4 (L4) - 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:

- Practices are "metrics-driven" and provide sufficient management insight (based on a quantitative understanding of

process capabilities) to predict optimal performance, ensure continued operations, and identify areas for improvement.
- Practices build upon established L3 maturity criteria and have 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.

L4 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 L4 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 data privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). This situational awareness is made possible through detailed metrics.*

SCR-CMM Level 5 (L5) - 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:
- Practices are “world-class” capabilities that leverage predictive analysis.
- Practices build upon established L4 maturity criteria and are time-sensitive to support operational efficiency, which likely includes automated actions through machine learning or Artificial Intelligence (AI).
- Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization.
- Process improvements are implemented according to “continuous improvement” practices to affect process changes.

L5 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. Interestingly, 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 required to be L5.

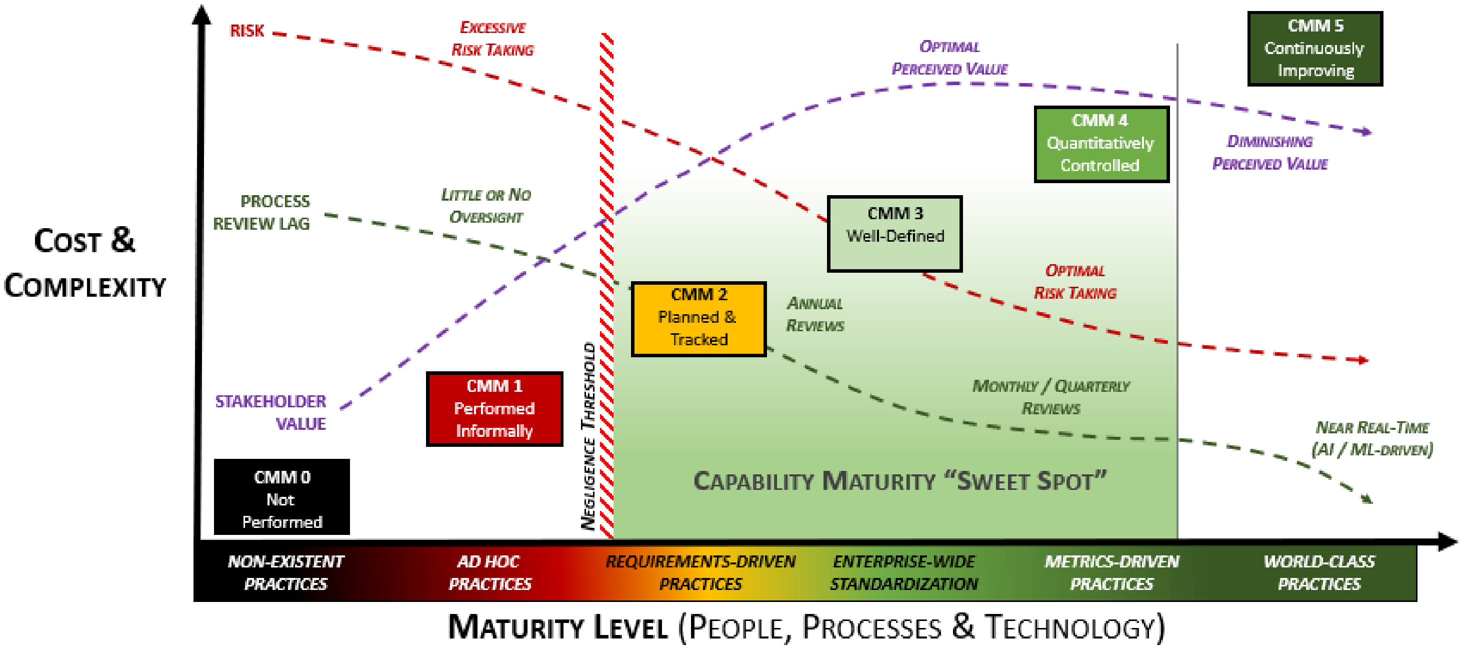
NOTE: The reality with a L5 level of maturity is often:
- *For small and medium-sized organizations, it is unrealistic to attain this level of maturity.*
- *For large organizations:*
    - *IT staff have clear requirements to implement standardized cybersecurity & privacy principles across the enterprise.*
    - *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 data 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 data 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 make 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 L2 and L4 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 data 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 data 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 SCR-CMM, a contributor identified an interesting insight that L0-L3 are "internal" maturity levels for cybersecurity and data privacy teams, whereas L4-L5 are "external" maturity levels that expand beyond those teams. When you look at the stakeholders involved in L0-L3, it is almost entirely IT, cybersecurity and data privacy. It isn't until L4-L5 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 L1 and L2. The reason for this is at L2, 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 L3. Oversight and process automation can decrease risk, but generally not as noticeably as steps taken to attain L3.

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

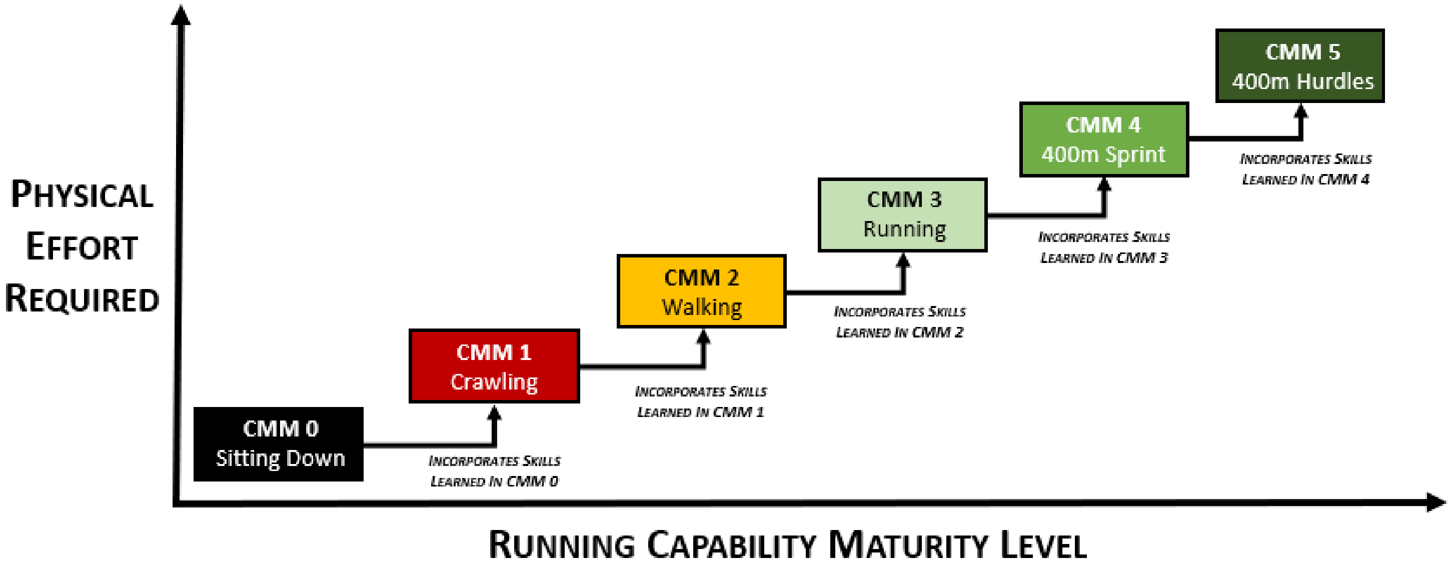
The perceived value of security controls increases with maturity. However, perceived value tends to decrease after L3 since the value of the additional cost and complexity becomes harder to justify to business stakeholders. Companies that are genuinely focused on being industry leaders are ideal candidates for L5 targets to support their aggressive business model needs.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

Analog Example – Sit / Crawl / Walk / Run / Sprint / Hurdle

The following example shows this approach being applied to the maturity levels for running, where it demonstrates the nested approach to the maturity levels by each succeeding level of maturity incorporates skills learned by the preceding level.

The point of this example is to demonstrate a relatable scenario that readers can comprehend how being asked to jump straight into an advanced level of maturity is not practical, where it requires some level of lesser maturity. For example, if you were just learning how to walk, it would be foolish to try and run the 400m hurdles that require both the strength and skill of sprinting, but also the knowledge of how to jump over an obstacle.



Physical Effort Required
CMM 0 Sitting Down
CMM 1 Crawling
CMM 2 Walking
CMM 3 Running
CMM 4 400m Sprint
CMM 5 400m Hurdles
Incorporates Skills Learned In CMM 0
Incorporates Skills Learned In CMM 1
Incorporates Skills Learned In CMM 2
Incorporates Skills Learned In CMM 3
Incorporates Skills Learned In CMM 4
Running Capability Maturity Level

In this example, this maturity model is applied to a control to raise an individual's resting heart rate through exercise.

- **L0 – Sitting Down**
  - Sitting down would be non-existent effort. No evidence of exercise exists.
  - Sitting down would be considered deficient in terms of meeting this control.
- **L1 – Crawling**
  - Crawling is at best considered ad-hoc exercise and likely doesn't meet the intent of the control.
  - Crawling would be considered deficient in terms of meeting this control.
- **L2 – Walking**
  - Walking builds on skills learned through crawling and demonstrates a capability that raises the individuals' resting heart rate.
  - Walking would meet the intent of the control, but there is clearly room for improvement.
- **L3 – Running**
  - Running builds on the skills learned through walking and meets the control's intent.
  - Running would be the "sweet spot" of maturity for this example.
- **L4 – 400-meter Sprint**
  - Sprinting builds on the skills learned through running and meets the control's intent.
  - Sprinting requires mastery of running skills to do it properly and avoid injury.
- **L5 – 400-meter Hurdles**
  - Running the hurdles builds upon skills learned through sprinting and meets the control's intent.
  - Hurdling requires a mastery of sprinting, since jumping hurdles is in addition to a sprinting race.

Maturity Model Use Cases

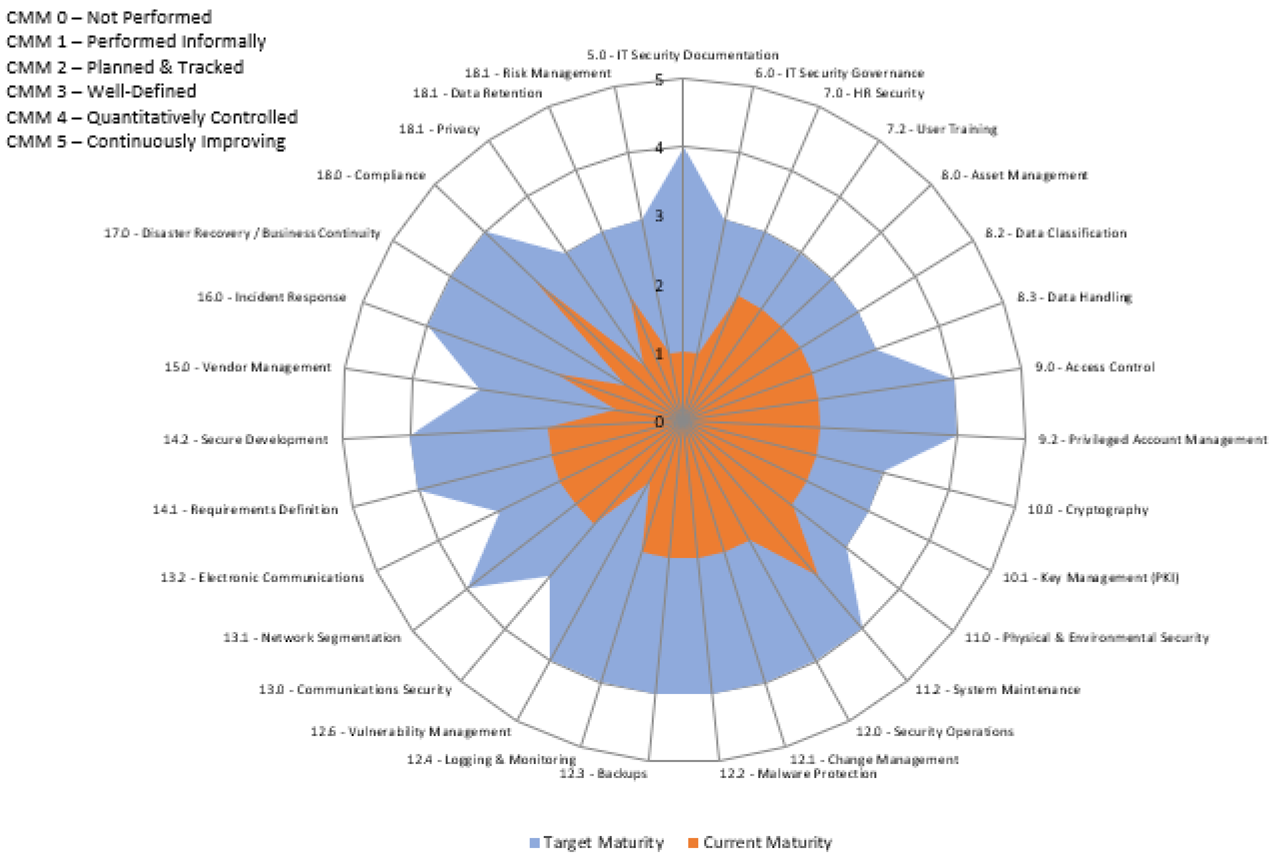
The SCR-CMM is meant to solve the problem of objectivity in both establishing and evaluating cybersecurity and data privacy controls. There are four (4) main objectives for the SCR-CMM:

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;
3. Provide minimum criteria that can be used to evaluate third-party service provider controls; and
4. Provide a means to perform due diligence of cybersecurity and data privacy practices as part of Mergers & Acquisitions (M&A).

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 data 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 SCR-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 PPTDF that are expected to exist 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 L3 and L4 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?”*** L3 maturity is generally considered “an environment that is in control” where it is well-managed, whereas being in a L4 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 L3 as the highest-level of maturity targets. Additionally, the cost to mature from a L3-4 or L4-5 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.

Identifying A Solution

The most efficient manner we can recommend would be to first look at the thirty-three (33) domains that make up the SCF and assign a high-level CMM level target for each domain.

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.

Use Case #2 – Assist Project Teams To Appropriately Plan & Budget Secure Practices

When you consider regulations such as the EU General Data Protection Regulation (GDPR), there is an expectation for systems, applications and processes to identify and incorporate cybersecurity and data privacy by default and by design. To determine what is appropriate and to evaluate it prior to “go live” it necessitates expectations for control maturity to be defined.

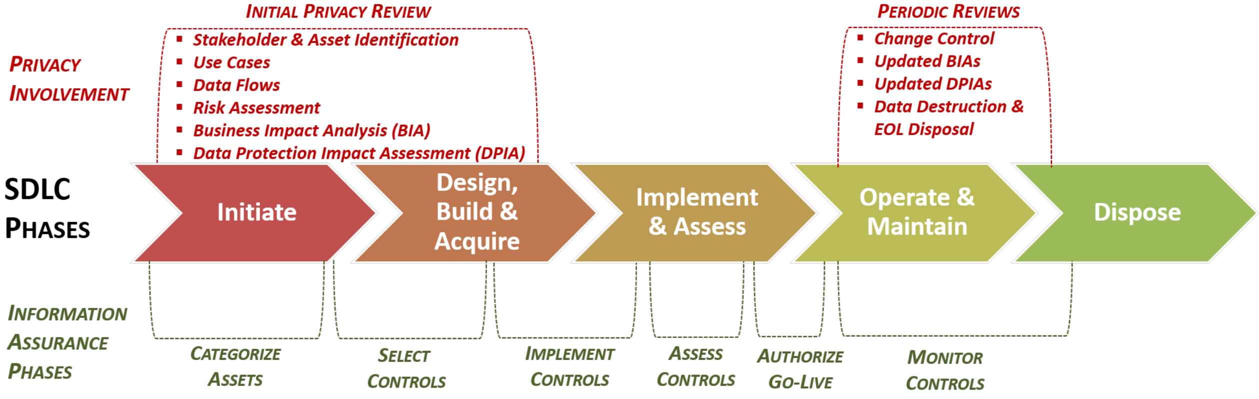
Identifying The Problem

In planning a project or initiative, it is important to establish “what right looks like” from cybersecurity and data protection 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

Referencing back to the SCR-CMM Overview section of this document, L0-1 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 L2-L4 to identify the reasonable people, processes and technologies that need to be incorporated into the solution.

As covered previously, 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 it is expected 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 L2-3 for planning purposes.

Identifying A Solution

While there are over 1,200 controls in the SCF's controls catalog, it is necessary for a project team to pare down that catalog to only what is applicable to the project (e.g., ISO 27002, PCI DSS, CCPA, etc.). This step simply involves filtering out the controls in the SCF that are not applicable. This step can also be done within Excel or within a GRC solution (e.g., SCF Connect, Cyturus, etc.). In the end, the result is a tailored set of controls that meets the project's specific needs.

Now that you have pared down the SCF's controls catalog to only what is applicable, it is a manual review process to identify the appropriate level of maturity for each of the controls. Ideally, the project will inherit the same target maturity level for controls as used throughout the organization. For any deviations, based on budget, time or other constraints, a risk assessment should be conducted to ensure a lower level of maturity for project-specific controls is appropriate.

Use Case #3 – Provide Objective Criteria To Evaluate Third-Party Service Provider Security

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

Identifying The Problem

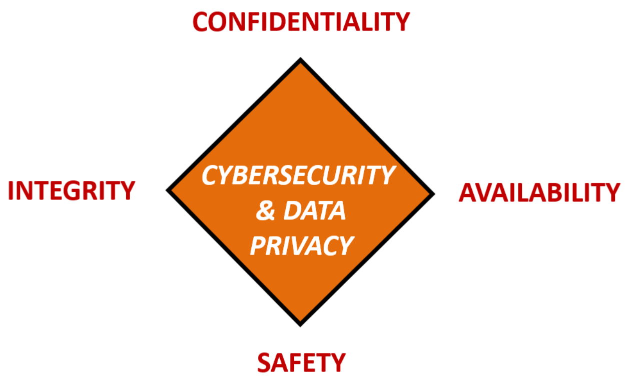
In managing a cybersecurity and data privacy program, it is important to address controls in a holistic manner, which includes governing the supply chain. ESPs are commonly considered the "soft underbelly" for an organization's security program, since ESP oversight has traditionally been weak or non-existent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

One of the issues with managing ESPs 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 ESP. The SCR-CMM can be used to obtain more nuanced answers from ESPs by having those ESPs select from L0-5 to answer if the control is implemented and how mature the process is.

Considerations

Referencing back to the SCR-CMM Overview section of this document, L0-1 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 L2-L4 to identify the reasonable people, processes and technologies that need ESPs 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 an ESP management perspective, this is often going to limit target CMM levels to L2-3 for most organizations.

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



Identifying A Solution

While there are over 1,200 controls in the SCF's controls catalog, it is necessary to pare down that catalog to only what is applicable to that specific ESP's scope of control (e.g., Managed Service Provider (MSP), Software as a Service (SaaS) provider, etc.). This step simply involves filtering out the controls in the SCF that are not applicable. This step can also be done within Excel or within a GRC solution (e.g., SCF Connect, Cyturus, etc.). In the end, the result is a tailored set of controls that address the ESP's specific aspects of the cybersecurity & privacy controls that it is responsible for or influences.

Now that you have pared down the SCF's controls catalog to only what is applicable, it is a manual review process to identify the appropriate level of maturity for each of the controls that would be expected for the ESP. Ideally, the ESP will inherit the same target maturity level for controls as used throughout the organization. For any deviations, based on contract clauses, budget, time or other constraints, a risk assessment should be conducted to ensure a lower level of maturity for ESP-specific controls is appropriate.

Use Case #4 – Due Diligence In Mergers & Acquisitions (M&A)

It is commonplace to conduct a cybersecurity and data privacy practices assessment as part of Mergers & Acquisitions (M&A) due diligence activities. The use of a gap assessment against a set of baseline M&A controls (e.g., SCF-B control set) can be used to gauge the level of risk. In practical terms, this type of maturity-based gap assessment can be used in a few ways:

- Sellers can provide the results from a first- or third-party gap assessment to demonstrate both strengths and weaknesses, as a sign of transparency.
- Buyers can identify unforeseen deficiencies that can:
  - Lead to a lower buying price; or
  - Backing out of the deal.

Identifying The Problem

Acquiring another entity involves a considerable amount of trust. Cybersecurity M&A due diligence exists to prevent the purchasing entity from potentially acquiring a class-action lawsuit or multi-million-dollar data protection-related fines (worst case scenarios). M&A is a game of cat and mouse between the two parties:

- The divesting entity is going to want to "put its best foot forward" and gloss over deficiencies; and
- The acquiring entity wants to know the truth about strengths and weaknesses.

If the acquiring entity only leverages a single framework (e.g., NIST CSF, ISO 27002 or NIST 800-53) for due diligence work, it will most likely provide a partial picture as to the divesting entity's cybersecurity and data privacy practices. That is why the SCF-B is a bespoke set of cybersecurity and data privacy controls that was purposely built for M&A to provide as complete a picture as possible about the divesting entity's cybersecurity and data privacy practices.

A control set questionnaire that asks for simple yes, no or not applicable answers is insufficient in M&A due diligence. Failure to leverage maturity-based criteria will result in the inability to provide critical insights into the actual security posture of the divesting entity. The SCR-CMM can be used to obtain more nuanced answers to determine (1) if a control is implemented and (2) how mature the process behind the control is.

Considerations

Referencing back to the SCR-CMM Overview section of this document, L0-1 levels of maturity are identified as being deficient from a "reasonable person perspective" in most cases. Therefore, acquiring entities need to look at the "capability maturity sweet spot" between L2-L4 to identify the reasonable people, processes and technologies needed to demonstrate to properly protect systems, applications, services and data, regardless of where it is stored, transmitted or processed.

Areas of deficiency can be identified and remediation costs determined, which can be used to adjust valuations. Key areas that affect valuations include, but are not limited to:

- Non-compliance with statutory, regulatory and/or contractual obligations;
- Data protection practices (e.g., privacy);
- IT asset lifecycle management (e.g., unsupported / legacy technologies);
- Historical cybersecurity incidents;
- Risk management (e.g., open items on a risk register or Plan of Action & Milestones (POA&M);
- Situational awareness (e.g., visibility into activities on systems and networks);
- Software licensing (e.g., intellectual property infringement);
- Business Continuity / Disaster Recovery (BC/DR);
- IT / cybersecurity architectures (e.g., deployment of on-premises, cloud and hybrid architectures); and

- IT /cybersecurity staffing competencies.

Identifying A Solution

The SCF did the hard work by developing the SCF-B control set. The "best practices" that comprise the SCF-B include:

- Trust Services Criteria (SOC 2);
- 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; and
- EU GDPR.

SECTION 10. SECURE, COMPLIANT & RESILIENT RISK MANAGEMENT MODEL (SCR-RMM)

To help simplify risk management practices, ComplianceForge and the SCF Council jointly developed the Secure, Compliant & Resilient Risk Management Model (SCR-RMM). The concept of creating the SCR-RMM was to establish an efficient methodology to identify, assess, report and mitigate risk across the entire organization.

The SCR-RMM:

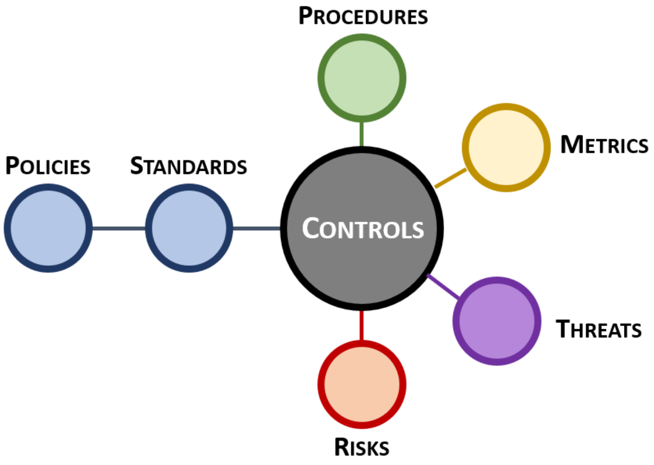
- Is a free solution that organizations can use to holistically approach that breaks risk management down into seventeen (17) distinctive steps;
- Exists is to help cybersecurity and data privacy functions create a repeatable methodology to identify, assess, report and mitigate risk;
- Offers flexibility to report on risk at a control level or aggregate level (e.g., a project, department, domain or organization-level); and
- Guides the decision to a risk treatment option (e.g., reduce, avoid, transfer or accept).

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

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

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

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



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

EXPERT INSIGHT (ROGUE RISK MANAGEMENT OPERATIONS): Cybersecurity teams “making up risks” points to a few security program governance issues:

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

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

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

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

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

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

Risk Management Discussion Protections

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

Before you read further, ask yourself these two (2) questions about your organization and your personal exposure in risk management:

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

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

Organizations often face conflicting expectations for risk management, based on department-level practices. For example, where disjointed risk management practices exist, a "Moderate Risk" often has entirely different financial and/or operational impacts across cybersecurity, IT, legal, finance, HR, operations, etc. The concept of Enterprise Risk Management (ERM) is to apply a comprehensive, organization-wide approach to risk management practices, where each department operates according to a similar playbook, where "Moderate Risk" means the same thing across the entire organization. This helps make an "apples to apples" comparison that can aid in creating a more holistic approach to risk management practices when risk designations are standardized.

Risk management activities are logical and systematic processes that can be used when making well-informed decisions to improve effectiveness and efficiency. Proactive risk management activities have these characteristics:

- Integrated into Business As Usual (BAU) activities (e.g., everyday work);
- Focuses on proactive management involvement, rather than reactive crisis management;
- Identifies and helps prepare for what might happen;

- Identifies opportunities to improve performance; and
- Proposes taking action to:
    - Avoid or reduce unwanted exposures; and/or
    - Maximize opportunities identified.

The articulation of risk management concepts is both an art and science. This requires a clear understanding of certain risk management terminology:

- Risk Appetite;
- Risk Tolerance; and
- Risk Threshold.

Risk management decisions must be explained in the context of the business, since risk management practices do not operate in a vacuum. Therefore, it is crucial to understand the environment where risk management practices exist. This also requires a clear understanding of business planning terminology:

- Mission;
- Vision; and
- Strategy.

From a hierarchical perspective:

- An organization's risk appetite exists at the corporate level to influence actions and decisions, specifically the organization's strategy. The strategy provides prioritization and resourcing constraints to the organization's various LOB.
- The risk appetite helps define the organization's risk tolerance to influence actions and decisions at the LOB level. Risk tolerance influences objectives, maturity targets and resource prioritization.
- Risk thresholds affect actions and decisions at the department and team levels. Risk thresholds influence processes, technologies, staffing levels and the supply chain (e.g., vendors, suppliers, consultants, contractors, etc.). Defined risk thresholds provide criteria to assess operational risks that exist in the course of conducting business.

It is acceptable for risk management practices to be:

- Quantifiable (objective);
- Qualifiable (subjective); or
- A hybrid approach that clearly identifies the subjective and object nature of risk analysis practices.

What is important to keep at the forefront of risk management considerations is the material nature of risk, as it pertains to the organization. Risks that have a material impact include, but are not limited to:

- Confidentiality, Integrity & Availability (CIA) of the organization's sensitive/regulated data;
- Supply chain security;
- Macroeconomic forces;
- Socio-political changes;
- Statutory / regulatory changes;
- Competitive landscape;
- Diplomatic sanctions (e.g., taxes, customs, embargoes, etc.); and
- Natural / manmade disasters (e.g., pandemics, war, etc.).

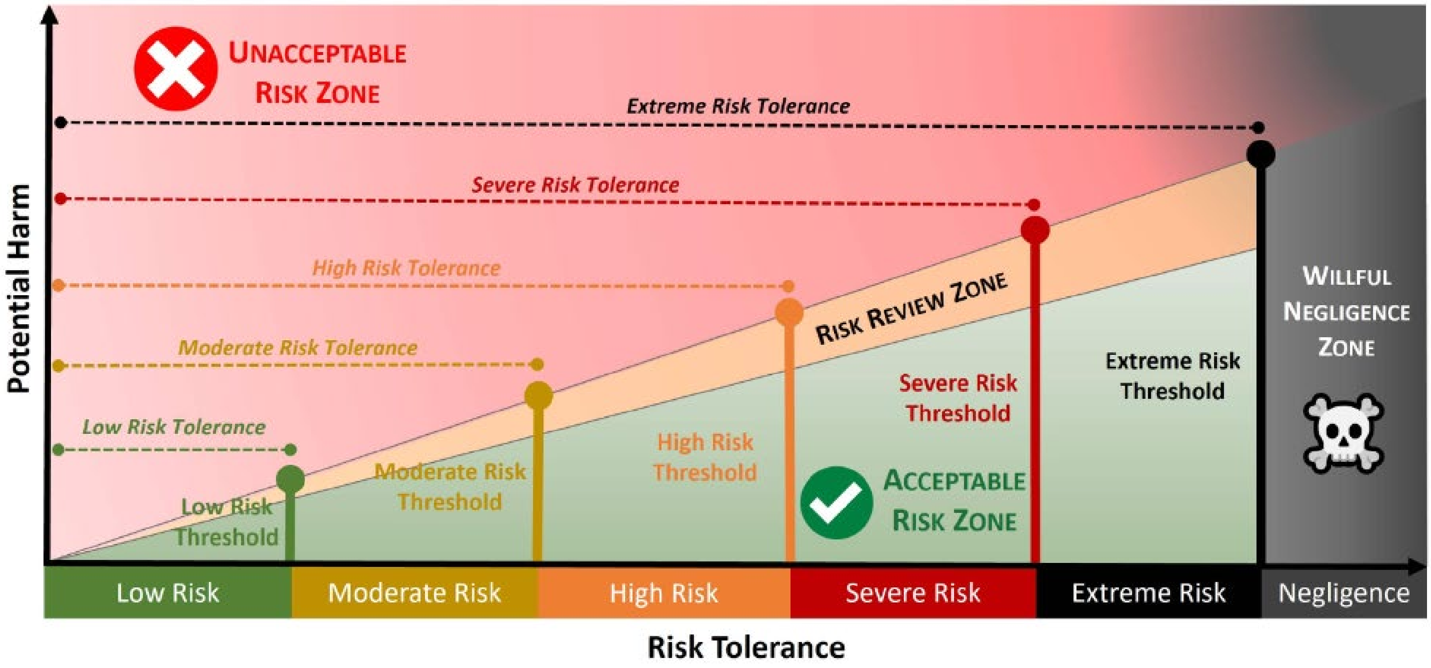
Baselining Risk Management Terminology

Risk management involves coordinated activities that optimize the management of potential opportunities and adverse effects. Proactive risk management activities provide a way to realize potential opportunities without exposing an organization to unnecessary peril.

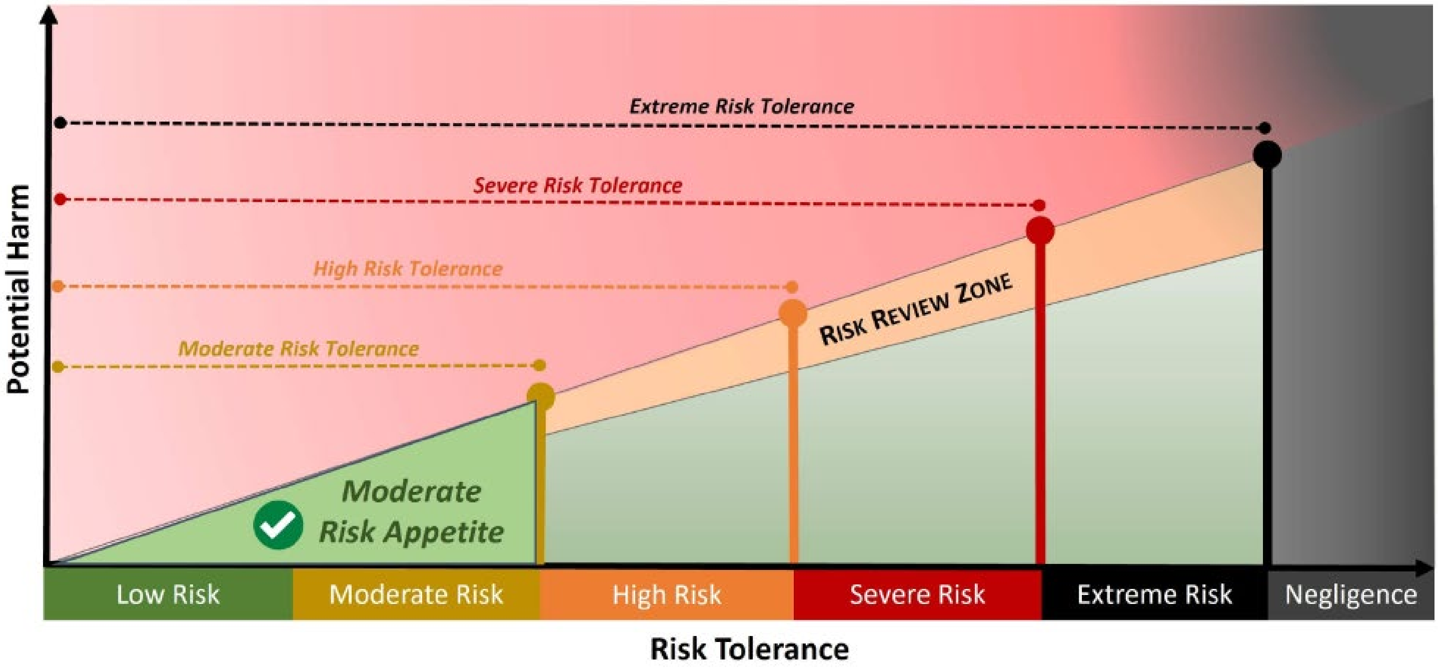
The goal of risk analysis is to determine the potential negative implications of an action or situation to determine one (1) of two (2) decisions:

1. **Acceptable Risk**: the criteria fall within a range of acceptable parameters; or
2. **Unacceptable Risk**: The criteria fall outside a range of acceptable parameters.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.



Building upon the graphic listed above, when viewed from a risk appetite perspective, for an organization that wants to follow a Moderate Risk Appetite, which establishes constraints for allowable and prohibited activities, based on the potential harm to the organization:



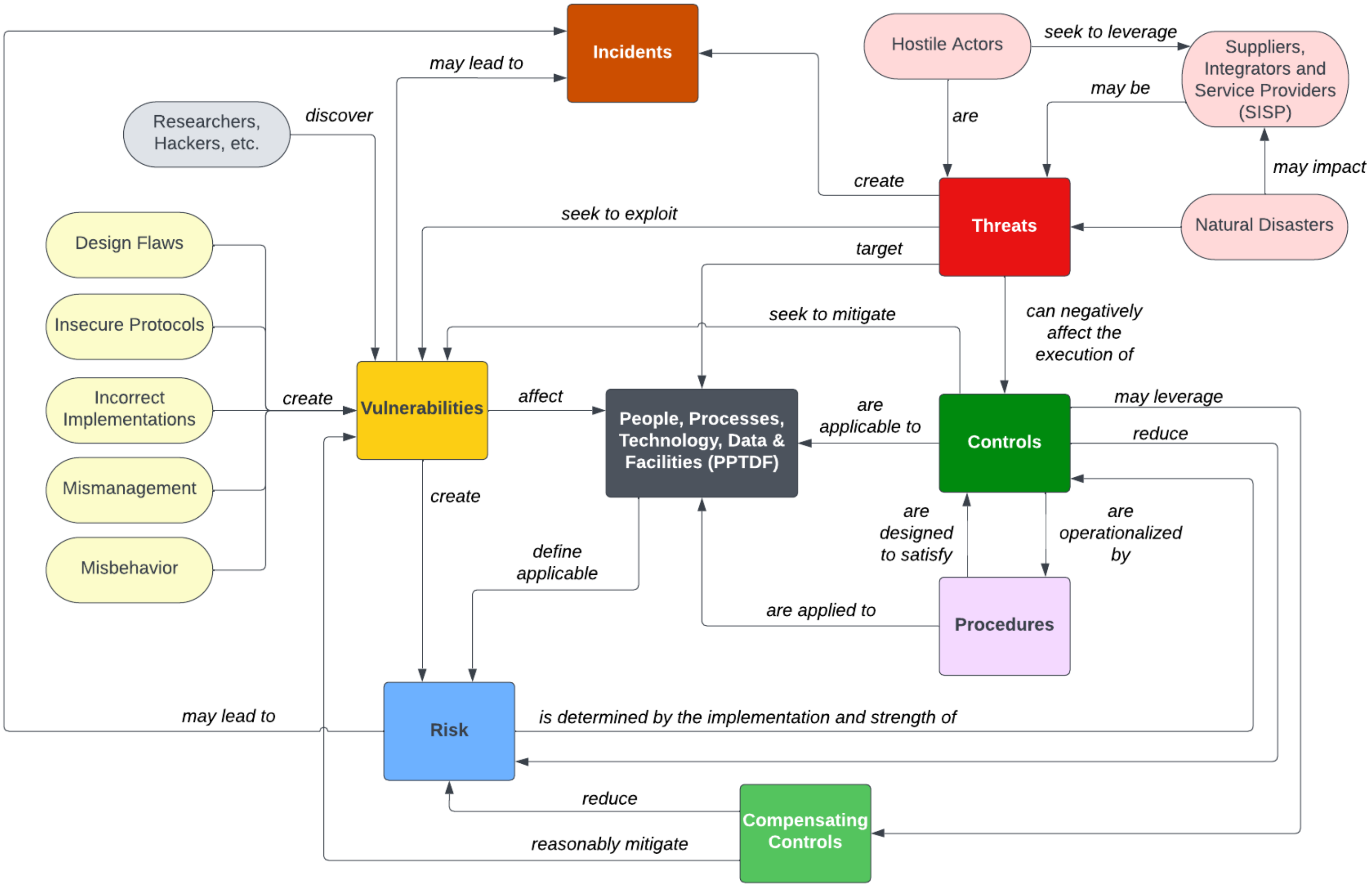
Understanding The Differences: Threats vs Vulnerabilities vs Risks

Risks and threats both tie into cybersecurity and data privacy controls, but it is important to understand the differences:

- A risk exists due to the absence of or a deficiency with a control; but
- A threat affects the ability of a control to exist or operate properly.

ComplianceForge published a "threats vs vulnerabilities vs risks" informational graphic that describes the relationship between these components. That informational graphic is shown below:[32]

[32] *Risk vs Threat vs Vulnerability Ecosystem - https://complianceforge.com/content/pdf/guide-risk-vs-threat-vs-vulnerability-ecosystem.pdf*



WHAT IS A RISK?

In the context of cybersecurity & data privacy practices, “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.*

WHAT IS A THREAT?

In the context of cybersecurity & data privacy practices, “threat” is defined as:

- Noun: *A person or thing likely to cause damage or danger.*
- Verb: *To indicate impending damage or danger.*

UNDERSTANDING THE DIFFERENCES BETWEEN: RISK TOLERANCE VS RISK THRESHOLD VS RISK APPETITE

Key concepts associated with risk management include:

- Risk Appetite: The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.[33]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a desired result. [34]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.[35]

[33] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*

[34] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*

[35] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*

What Is A Risk Appetite?

A risk appetite is a broad "risk management concept" that is used to inform employees about what is and is not acceptable, in terms of risk management from an organization's executive leadership team.

A risk appetite does not contain granular risk management criteria and is primarily a "management statement" that is subjective in nature. Similar in concept to how a policy is a *"high-level statement of management intent,"* an organization's defined risk appetite is a high-level statement of how all, or certain types of, risk are willing to be accepted.

Examples of an organization stating its risk appetite from basic to more complex statements:

- *"[organization name] is a low-risk organization and will avoid any activities that could harm its customers."*
- *"[organization name] will aggressively pursue innovative solutions through Research & Development (R&D) to provide industry-leading products and services to our clients, while maintaining a Moderate Risk Appetite. Developing breakthrough products and services does invite potential risk through changes to traditional supply chains, disruptions to business operations and changing client demand. Proposed business practices that pose greater than a Moderate Risk will be considered on a case-by-case basis for financial, operational and legal implications."*

It is important to point out that in many immature risk programs, risk appetite statements are divorced from reality. Executive leaders mean well when they issue risk appetite statements, but the Business As Usual (BAU) practices routinely violate the risk appetite. This is often due to numerous reasons that include, but are not limited to:

- Technical debt;
- Dysfunctional management decisions;
- Insecure practices;
- Inadequate funding/resourcing;
- Improperly scoped support contracts (e.g., Managed Service Providers (MSPs), consultants, vendors, etc.); and
- Lack of pre-production security testing.

What Is A Risk Tolerance?

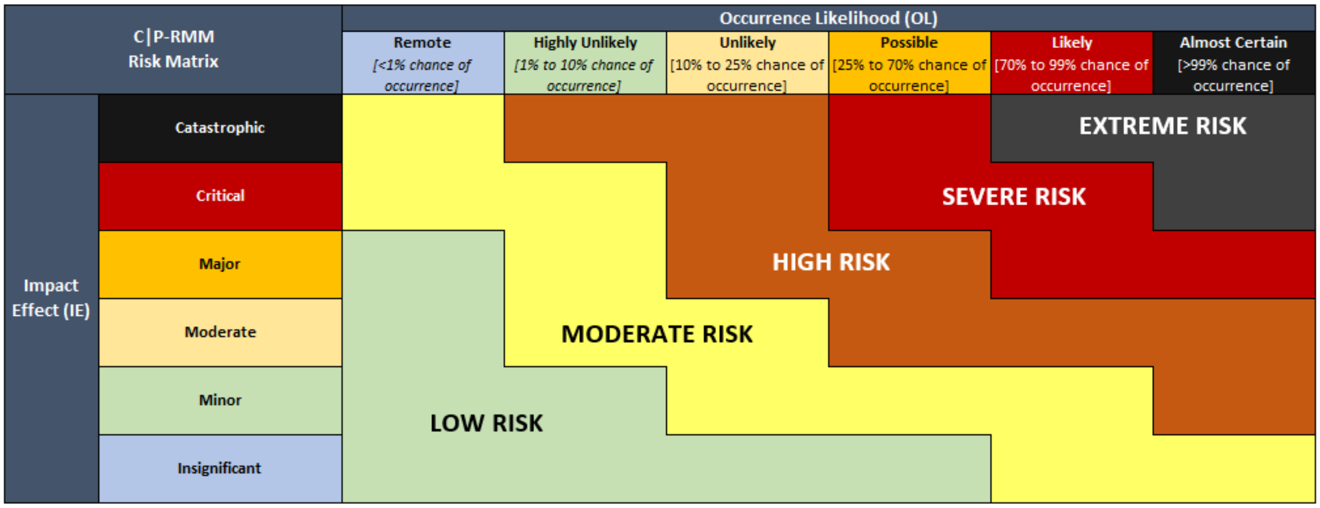
Risk tolerance is based on objective criteria, unlike the subjective, conceptual nature of a risk appetite. Defining objective criteria is a necessary step to be able to categorize risk on a graduated scale. Establishing objective criteria to quantify the impact of a risk enables risk assessments to leverage that same criteria and assist decision-makers in their risk management decisions (e.g., accept, mitigate, transfer or avoid).

From a graduated scale perspective, it is possible to define "tolerable" risk criteria to create five (5) useful categories of risk:

1. Low Risk;
2. Moderate Risk;
3. High Risk;
4. Severe Risk; and
5. Extreme Risk.

There are two (2) objective criteria that go into defining what constitutes a low, moderate, high, severe or Extreme Risk includes:

1. Impact Effect (IE); and
2. Occurrence Likelihood (OL).


C|P-RMM
Risk Matrix
Occurrence Likelihood (OL)
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]
Impact Effect (IE)
Catastrophic
Critical
Major
Moderate
Minor
Insignificant
EXTREME RISK
SEVERE RISK
HIGH RISK
MODERATE RISK
LOW RISK

The six (6) categories of IE are:

1. Insignificant *(e.g., organization-defined little-to-no impact to business operations);*
2. Minor *(e.g., organization-defined minor impacts to business operations)*;
3. Moderate *(e.g., organization-defined moderate impacts to business operations)*;
4. Major *(e.g., organization-defined major impacts to business operations)*;
5. Critical *(e.g., organization-defined critical impacts to business operations)*; and
6. Catastrophic *(e.g., organization-defined catastrophic impacts to business operations).*

The six (6) categories of OL are:

1. Remote possibility *(e.g., <1% chance of occurrence)*;
2. Highly unlikely *(e.g., from 1% to 10% chance of occurrence)*;
3. Unlikely *(e.g., from 10% to 25% chance of occurrence)*;
4. Possible *(e.g., from 25% to 70% chance of occurrence)*;
5. Likely *(e.g., from 70% to 99% chance of occurrence)*; and
6. Almost certain *(e.g., >99% chance of occurrence)*.

There are three (3) general approaches are commonly employed to estimate OL:

1. Relevant historical data;
2. Probability forecasts; and
3. Expert opinion.

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

- Statutory, regulatory and contractual compliance obligations (including adherence to privacy principles for ethical data protection practices).
- Organization-specific threats (natural and manmade).
- Reasonably expected industry practices.
- Pressure from competition.
- Executive management decisions.

Low Risk Tolerance

Organizations that would be reasonably expected to adopt a Low Risk Tolerance generally:

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

Organizations that are reasonably expected to operate with a Low Risk Tolerance include, but are not limited to:

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

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

Moderate Risk Tolerance

Organizations that would be reasonably expected to adopt a Moderate Risk Tolerance generally:

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

Organizations that are reasonably expected to operate with a Moderate Risk Tolerance include, but are not limited to:

- Education (e.g., K-12, colleges, universities, etc.)
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.)
- Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, etc.)
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.)
- Technology services (e.g., Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), etc.)
- Manufacturing (high value)
- Healthcare
- Defense Industrial Base (DIB) contractors and subcontractors
- Legal services (e.g., law firms)
- Construction (high value)

High Risk Tolerance

Organizations that would be reasonably expected to adopt a High Risk Tolerance generally:

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

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups
- Hospitality industry (e.g., restaurants, hotels, etc.)
- Construction
- Manufacturing
- Personal services

Severe Risk Tolerance

Organizations that would be reasonably expected to adopt a Severe Risk Tolerance generally:

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

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups
- Artificial Intelligence (AI) developers

Extreme Risk Tolerance

Organizations that would be reasonably expected to adopt an Extreme Risk Tolerance generally:

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

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

- Artificial Intelligence (AI) developers

What Is A Risk Threshold?

Risk thresholds are directly tied to risk tolerance and utilize organization-specific criteria (e.g., acceptable and unacceptable parameters). These risk thresholds exist between the different levels of risk tolerance (e.g., between Low Risk and Moderate Risk, between Moderate Risk and High Risk, etc.). By establishing these risk thresholds, it brings the "graduated scale perspective" to life for risk management practices. Risk thresholds are criteria that are unique to an organization:

- Organization-specific activities / scenarios that could damage the organization’s reputation;
- Organization specific activities / scenarios that could negatively affect short-term and long-term profitability; and
- Organization specific activities / scenarios that could impede business operations.

Risk thresholds are entirely unique to each organization, based on several factors that include:

- Financial stability;
- Management preferences;
- Compliance obligations (e.g., statutory, regulatory and/or contractual); and
- Insurance coverage limits.

What Is Materiality?

The SCF defines materiality as, *“A deficiency, or a combination of deficiencies, in an organization’s cybersecurity and/or data privacy controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance.”*[36]

The intended usage of materiality is meant to provide relevant context, as it pertains to risk thresholds. This is preferable when compared to relatively hollow risk findings that act more as guidelines than actionable, decision-making criteria. Cybersecurity materiality is meant to act as a "guard rail" for risk management decisions. A material weakness crosses an organization’s risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

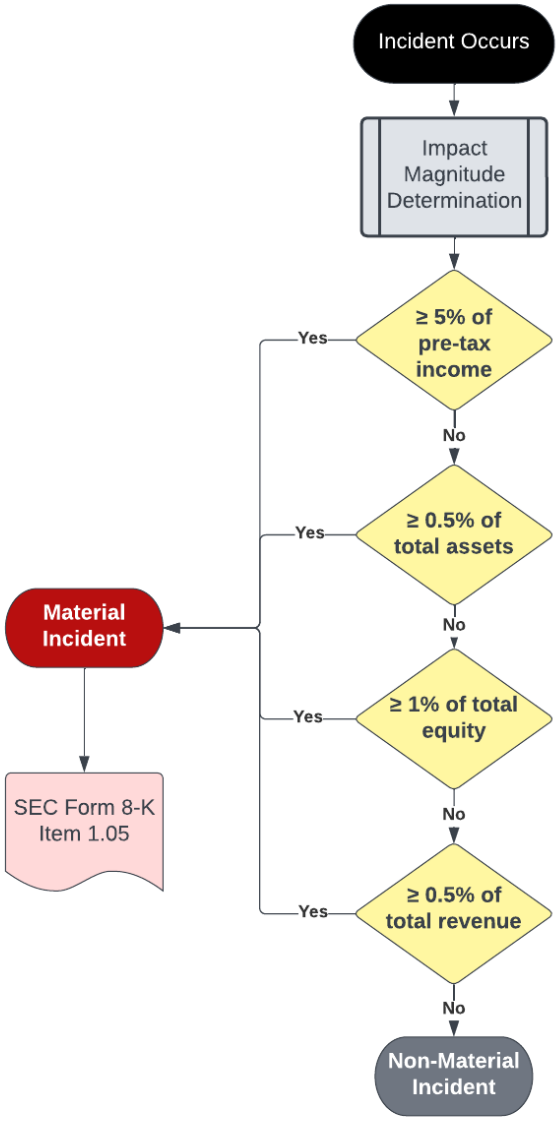
The SEC, Generally Accepted Accounting Principles (GAAP) and International Financial Reporting Standards (IFRS) lack specificity in defining the criteria for materiality. Therefore, organizations generally have leeway to define it on their own. The lack of authoritative definition for materiality is not unique, since the concept of risk appetite, risk tolerance and risk threshold also suffer from nebulous definitions by statutory and regulatory authorities.

For an item to be considered material, the control deficiency, risk, threat or incident (singular or a combination) generally must meet one or more of the following criteria where the potential financial impact is:[37]

- ≥ 5% of pre-tax income
- ≥ 0.5% of total assets
- ≥ 1% of total equity (shareholder value); and/or
- ≥ 0.5% of total revenue.

This materiality determination can be visualized with this infographic with the callout for publicly traded companies having a requirement to publicly disclose material cybersecurity incidents: [38]

[36] *SCF Cybersecurity Materiality - https://securecontrolsframework.com/cybersecurity-materiality/*
[37] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*
[38] *SEC Cybersecurity Final Rule - https://www.sec.gov/files/rules/final/2023/33-11216.pdf*



Historical Context For Cybersecurity & Data Privacy Materiality Usage

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

- Per the Security and Exchange Commission (SEC), information is material *"to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered."*[39]
- Per the International Accounting Standards Board (IASB), information is material, *"if omitting, misstating or obscuring it could reasonably be expected to influence the decisions that the primary users of general purpose financial statements make on the basis of those financial statements, which provide financial information about a specific reporting entity."*[40]

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

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

[39] *SEC - https://www.sec.gov/comments/265-24/26524-77.pdf*
[40] *IFRS - https://www.ifrs.org/content/dam/ifrs/project/definition-of-materiality/definition-of-material-feedback-statement.pdf*

Risk Management Options

Traditional risk management practices have four (4) options to address identified risk:

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

In a mature risk program, the results of risk assessments are evaluated with the organization's risk appetite in consideration. For example, if the organization has a Moderate Risk Appetite and there are several findings in a risk assessment that are High Risk, then action must be taken to reduce the risk. Accepting a High Risk would violate the Moderate Risk Appetite set by management. In reality, which leaves remediation, transferring or avoiding as the remaining three (3) options, since accepting the risk would be prohibited.

Practical Risk Management Example

For an example scenario, a theoretical company is experimenting with Artificial Intelligence (AI) to strengthen its products and/or services. Its long-standing risk appetite is relatively conservative, where the company draws a hard line that any risk over Moderate is unacceptable. Additionally, the company has zero tolerance for any activities that could harm its customers (e.g., physically or financially).

Given the necessary changes to ramp up both talent and technology to put the appropriate solutions in place to meet the company's deadlines, there are gaps/deficiencies. When the risk management team assesses the associated risks, the results identify a range of risks from High to Extreme. The reason for these results is simply due to the higher likelihood of emergent behaviors occurring from AI that potentially could harm individuals (e.g., catastrophic impact effect). The results were objective and told a compelling story that there is a realistic chance of significant damage to the company's reputation and financial liabilities from class action lawsuits.

With those results that point to risks exceeding the organization's risk appetite, it is a management decision on how to proceed. What does the CEO / Board of Directors (BoD) do?

- Dispense with its long-standing risk appetite for this specific project so that a potentially lucrative business opportunity can exist?
- Is the AI project cancelled due to the level of risk?
- If the CEO/BoD proceeds with accepting the risk, is it violating its fiduciary duties, since it is accepting risk that it previously deemed unacceptable? Additionally, would it be considered negligent to accept high, severe or Extreme Risk (e.g., would a rational individual under similar circumstances make the same decision?)?

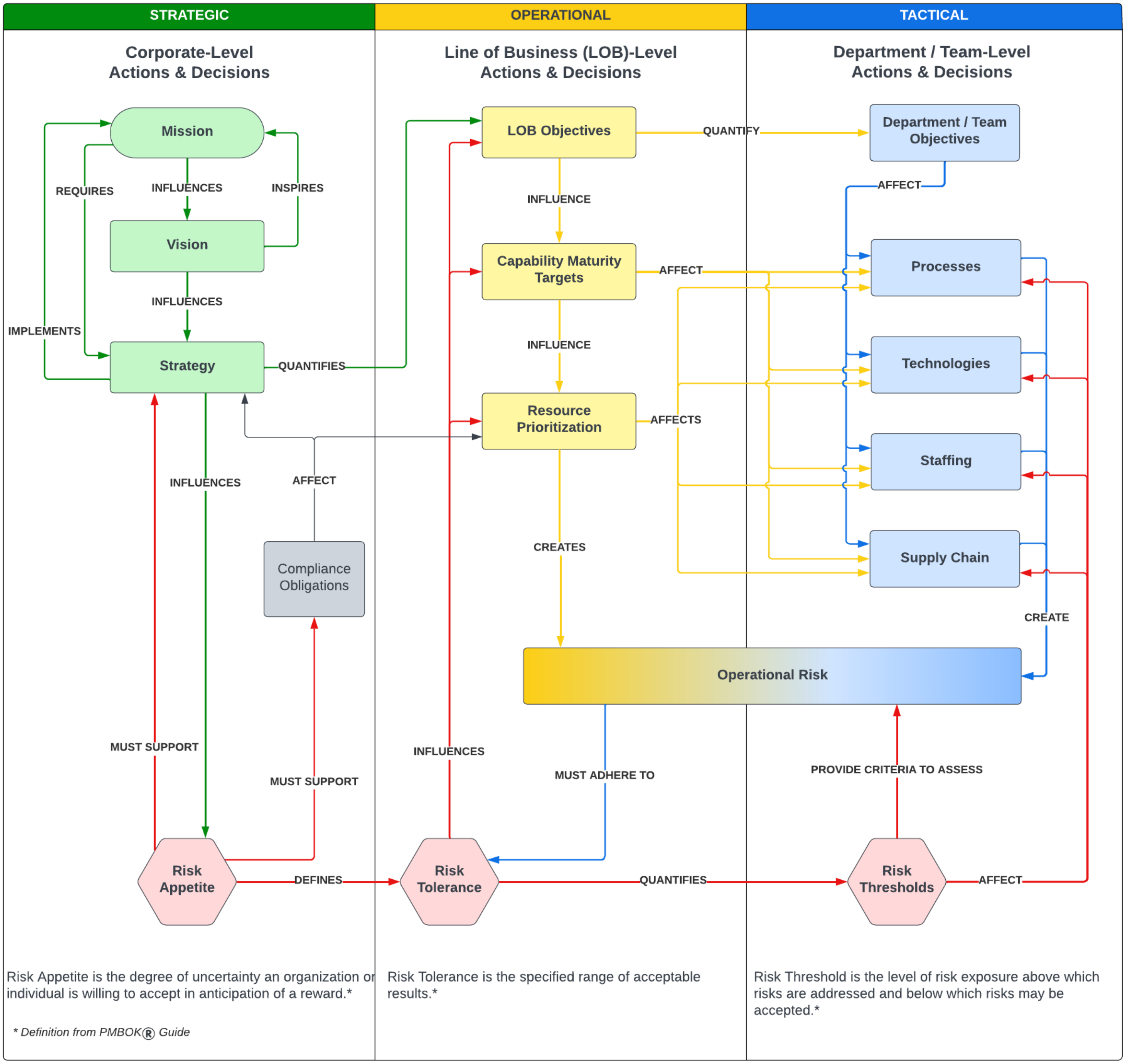
These are all very real topics that need to be considered and how risk is managed has significant legal and financial implications.

Summarizing The Integration Of Risk Management & Business Planning

These key concepts of how risk appetite, risk tolerance and risk thresholds interact with strategic, operational and tactical actions and decisions can be visualized in the following graphic:[41]

- At the strategic layer, where corporate-level actions and decisions are made, the organization's risk appetite is defined. The scope of the risk appetite can be organization-wide or compartmentalized to provide enhanced granularity.
- At the operational level, where Line of Business (LOB)-level actions and decisions are made, the organization's risk tolerance is put into practice. The organization's risk tolerance is defined by its established risk appetite.
- At the tactical level, where department / team-level actions and decisions are made, the organization's risk thresholds are used to provide criteria to assess operational risk. That operational risk must adhere to the organization's risk tolerance and therefore, its risk appetite.

[41] *Strategic vs Operational vs Tactical Risk Management - https://complianceforge.com/content/Risk-Appetite-vs-Risk-Tolerance-vs-Risk-Thresholds.pdf*



Risk Appetite is the degree of uncertainty an organization or individual is willing to accept in anticipation of a reward.*

Risk Tolerance is the specified range of acceptable results.*

Risk Threshold is the level of risk exposure above which risks are addressed and below which risks may be accepted.*

** Definition from PMBOK® Guide*

[graphic download - https://complianceforge.com/content/Risk-Appetite-vs-Risk-Tolerance-vs-Risk-Thresholds.pdf]

Risk Management: Strategic Considerations

At this level, corporate-level actions and decisions define the strategic direction of the organization and its approach to risk management practices:

Mission

- Influences the vision of the organization.
- Requires a strategy to accomplish.

Vision

- Inspires personnel to achieve the mission.

Strategy

- Implements the mission.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

- Quantifies “downstream” objectives for Lines of Business (**LOB**)
- Influences the organization’s risk appetite.

Compliance Obligations

- Affect the strategy.
- Affect resource prioritization.

Risk Appetite

- Must support the organization’s strategy.
- Defines the organization’s risk tolerance.

Risk Management: Operational Considerations

At this level, Line of Business (LOB)-level actions and decisions define the operational management of the organization:

Line of Business (LOB) Objectives

- Are quantified and prioritized by the organization’s strategy.
- Influence necessary capability maturity targets.
- Quantifies “downstream” objectives at the department / team level.

Capability Maturity Targets

- Are influenced by LOB objectives.
- Influences resource prioritization.
- Affects:
  - Processes that are implemented to achieve objectives;
  - Technologies used to support operations;
  - Staffing levels at the department / team level; and
  - Supply chain quality & security (e.g., vendors, suppliers, contractors, consultants, etc.).

Resource Prioritization

- Creates operational risks.
- Affects:
  - Processes that are implemented to achieve objectives;
  - Technologies used to support operations;
  - Staffing levels at the department / team level; and
  - Supply chain quality & security (e.g., vendors, suppliers, contractors, consultants, etc.).

Risk Tolerance

- Is defined by the organization’s risk appetite.
- Influences LOB objectives.
- Quantifies the organization’s risk thresholds.

Risk Management: Tactical Considerations

At this level, department / team-level actions and decisions define the tactics used for day-to-day operations:

Department / Team Objectives

- Are quantified and prioritized by LOB objectives.
- Affect:
  - Processes that are implemented to achieve objectives;
  - Technologies used to support operations;
  - Staffing levels at the department / team level; and
  - Supply chain quality & security (e.g., vendors, suppliers, contractors, consultants, etc.).

Processes

- Are affected by:
  - Department / team objectives;
  - Capability maturity targets; and

    - Resource prioritization.
- Create operational risks.

Technologies

- Are affected by:
    - Department / team objectives;
    - Capability maturity targets; and
    - Resource prioritization.
- Create operational risks.

Staffing

- Are affected by:
    - Department / team objectives;
    - Capability maturity targets; and
    - Resource prioritization.
- Creates operational risks.

Supply Chain

- Are affected by:
    - Department / team objectives;
    - Capability maturity targets; and
    - Resource prioritization.
- Creates operational risks.

Risk Thresholds

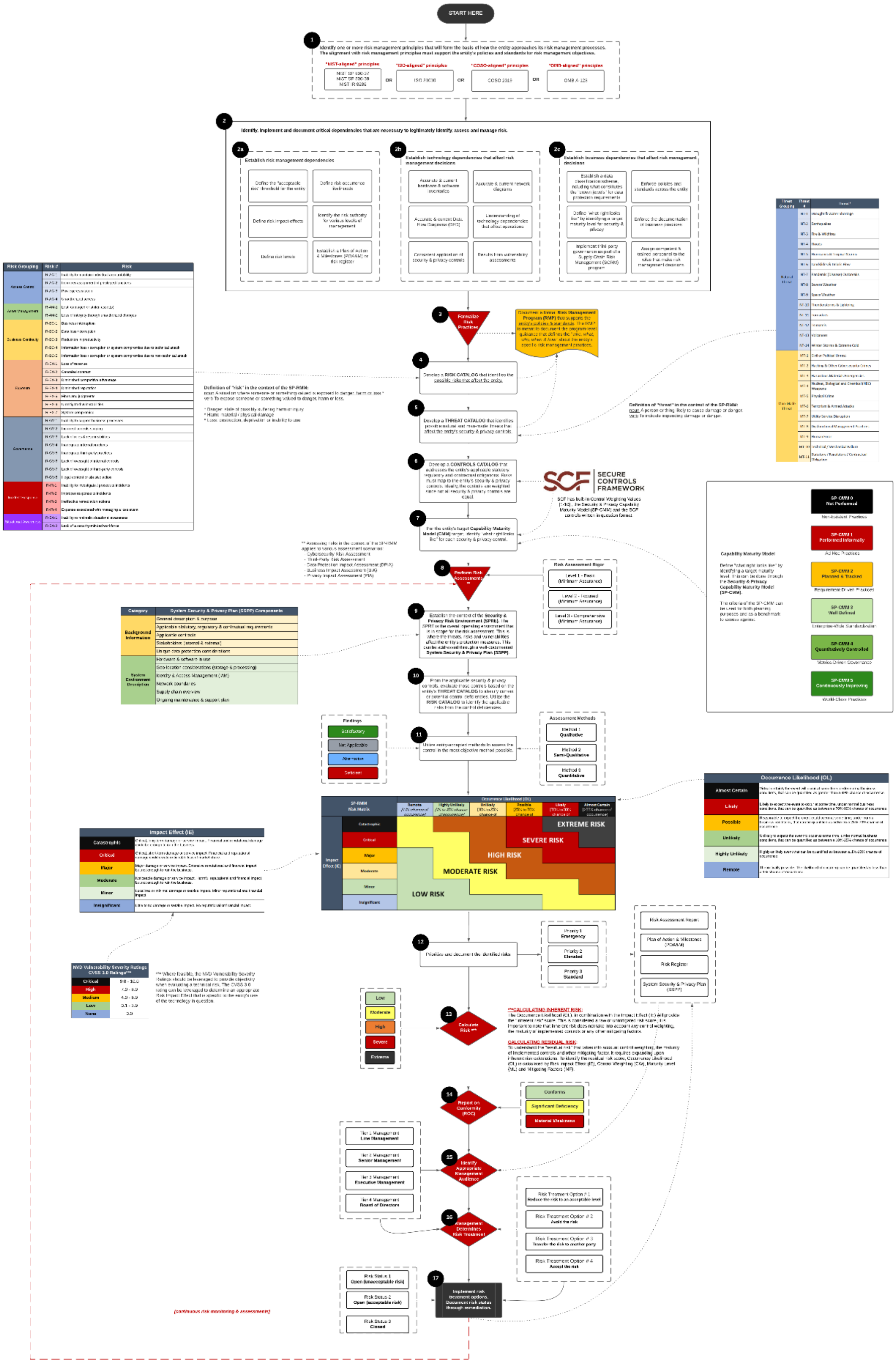
- Provide criteria to assess operational risks.
- Affect:
    - Processes that are implemented to achieve objectives;
    - Technologies used to support operations;
    - Staffing levels at the department / team level; and
    - Supply chain quality & security (e.g., vendors, suppliers, contractors, consultants, etc.).

Operational Risk

- Is assessed against the organization’s risk thresholds.
- Must adhere to the organization’s risk tolerance, where the organization has four (4) options to address identified risks:
    1. Reduce the risk to an acceptable level;
    2. Avoid the risk;
    3. Transfer the risk to another party; or
    4. Accept the risk.

Using The SCR-RMM

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


START HERE
1
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.
"NIST-aligned" principles
NIST SP 800-37
NIST SP 800-39
NIST IR 8286
OR
"ISO-aligned" principles
ISO 31010
OR
"COSO-aligned" principles
COSO 2013
OR
"OMB-aligned" principles
OMB A-123
2
Identify, implement and document critical dependencies that are necessary to legitimately identify, assess and manage risk.
2a
Establish risk management dependencies
Define the "acceptable risk" threshold for the entity
Define risk occurrence likelihoods
Define risk impact effects
Identify the risk authority for various levels of management
Define risk levels
Establish a Plan of Action & Milestones (POA&M) or risk register
2b
Establish technology dependencies that affect risk management decisions
Accurate & current hardware & software inventories
Accurate & current network diagrams
Accurate & current Data Flow Diagrams (DFD)
Understanding of technology dependencies that affect operations
Consistent application of security & privacy controls
Results from vulnerability assessments
2c
Establish business dependencies that affect risk management decisions
Establish a data classification scheme, including what constitutes the "crown jewels" for data protection requirements
Enforce policies and standards across the entity
Define "what right looks like" by identifying a target maturity level for security & privacy
Enforce the documentation of business practices
Implement third-party governance as part of a Supply Chain Risk Management (SCRM) program
Assign competent & trained personnel to the roles that make risk management decisions
3
Formalize Risk 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
Develop a RISK CATALOG that identifies the possible risks that affect the entity.
Definition of "risk" in the context of the SP-RMM:
5
Develop a THREAT CATALOG that identifies possible natural and man-made threats that affect the entity's security & privacy controls.
Definition of "threat" in the context of the SP-RMM:
Risk Grouping
Risk #
Risk
Threat Grouping
Threat #
Threat*
Natural Threat
Man-Made Threat
6
Develop a CONTROLS CATALOG 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.
SCF SECURE CONTROLS FRAMEWORK
SCF has built-in Control Weighting Values (1-10), the Security & Privacy Capability Maturity Model (SP-CMM) and the SCF controls written in question format.
7
For the entity's target Capability Maturity Model (CMM) target, identify "what right looks like" for each security & privacy control.
Capability Maturity Model
Define "what right looks like" by identifying a target maturity level. This can be done through the Security & Privacy Capability Maturity Model (SP-CMM).
The criteria of the SP-CMM can be used for both planning purposes and as a benchmark to assess against.
SP-CMM 0
Not Performed
Non-Existent Practices
SP-CMM 1
Performed Informally
Ad Hoc Practices
SP-CMM 2
Planned & Tracked
Requirement-Driven Practices
SP-CMM 3
Well Defined
Enterprise-Wide Standardization
SP-CMM 4
Quantitatively Controlled
Metrics-Driven Governance
SP-CMM 5
Continuously Improving
World-Class Practices
8
Perform Risk Assessments **
Risk Assessment Rigor
Level 1 - Basic (Minimum Assurance)
Level 2 - Focused (Minimum Assurance)
Level 3 - Comprehensive (Minimum Assurance)
9
Establish the context of the Security & Privacy Risk Environment (SPRE). The SPRE is the overall operating environment that is in scope for the risk assessment. This is where the threats, risks and vulnerabilities affect the entity's protection measures. This can be addressed through a well-documented System Security & Privacy Plan (SSPP).
Category
System Security & Privacy Plan (SSPP) Components
Background Information
System Environment Description
10
From the applicable security & privacy controls, evaluate those controls based on the entity's THREAT CATALOG to identify current or potential control deficiencies. Utilize the RISK CATALOG to identify the applicable risks from the control deficiencies.
11
Utilize entity-accepted methods to assess the control in the most objective method possible.
Findings
Satisfactory
Not Applicable
Alternative
Deficient
Assessment Methods
Method 1
Qualitative
Method 2
Semi-Qualitative
Method 3
Quantitative
SP-RMM Risk Matrix
Occurrence Likelihood (OL)
Remote
Highly Unlikely
Unlikely
Possible
Likely
Almost Certain
Impact Effect (IE)
Catastrophic
Critical
Major
Moderate
Minor
Insignificant
EXTREME RISK
SEVERE RISK
HIGH RISK
MODERATE RISK
LOW RISK
Occurrence Likelihood (OL)
Almost Certain
Likely
Possible
Unlikely
Highly Unlikely
Remote
Impact Effect (IE)
Catastrophic
Critical
Major
Moderate
Minor
Insignificant
NVD Vulnerability Severity Ratings CVSS 3.0 Ratings**
Critical 9.0 - 10.0
High 7.0 - 8.9
Medium 4.0 - 6.9
Low 0.1 - 3.9
None 0.0
12
Prioritize and document the identified risks
Priority 1
Emergency
Priority 2
Elevated
Priority 3
Standard
Risk Assessment Report
Plan of Action & Milestones (POA&M)
Risk Register
System Security & Privacy Plan (SSPP)
13
Calculate Risk ***
Low
Moderate
High
Severe
Extreme
***CALCULATING INHERENT RISK:
CALCULATING RESIDUAL RISK:
14
Report on Conformity (ROC)
Conforms
Significant Deficiency
Material Weakness
15
Identify Appropriate Management Audience
Tier 1 Management
Line Management
Tier 2 Management
Senior Management
Tier 3 Management
Executive Management
Tier 4 Management
Board of Directors
16
Management Determines Risk Treatment
Risk Treatment Option # 1
Reduce the risk to an acceptable level
Risk Treatment Option # 2
Avoid the risk
Risk Treatment Option # 3
Transfer the risk to another party
Risk Treatment Option # 4
Accept the risk
17
Implement risk treatment options. Document risk status through remediation.
Risk Status 1
Open (unacceptable risk)
Risk Status 2
Open (acceptable risk)
Risk Status 3
Closed
[continuous risk monitoring & assessment]

[graphic download - https://securecontrolsframework.com/content/SCF-Risk-Management-Model-Calculations.pdf]

The SCR-RMM is broken down into seventeen (17) primary steps:

SCR-RMM Step 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; and
- OMB A-123.

SCR-RMM Step 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:

SCR-RMM Step 2A. Risk Management Dependencies

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

- Define the “acceptable risk” threshold for your entity;
- Define risk Occurrence Likelihood (OL);
- Define risk Impact Effect (IE);
- Define risk levels;
- Define the various levels of entity management who can “sign off” on risk levels; and
- Establish a Plan of Action & Milestones (POA&M), risk register or some other method to track risks from identification through remediation.

SCR-RMM Step 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 cybersecurity and data privacy controls across the organization; and
- Maintain situational awareness of technology-related assets across the organization (e.g., vulnerability scanning & patch management levels).

SCR-RMM Step 2C. Business Dependencies

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

- A data classification scheme needs to exist that is consistent across the organization, including an understanding of what constitutes the “crown jewels” of that require enhanced data protection requirements;
- Business leadership needs to dictate the technological 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 cybersecurity and data privacy controls;
- A multi-discipline effort is needed to establish and maintain a Supply Chain Risk Management (SCRM) program that governs the organization’s supply chain. This requires legal, procurement, security, privacy and Line of Business (LOB) involvement;
- Policies and standards must be uniformly applied across the organization;
- LOB management needs to ensure its project teams properly document business practices and provide that information to technology, cybersecurity and data 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); and
- Since the LOB “owns” risk management decisions, the organization needs to ensure that those individuals in roles that make risk management decisions are competent and appropriately trained to make risk-related decisions.

SCR-RMM Step 3. Formalize Risk Management Practices

Document a formal Risk Management Program (RMP) that supports the entity's policies & standards. The RMP is meant to:

- Reference the most appropriate industry frameworks to provide a comprehensive and holistic approach to identifying, managing and remediating risks;
- Incorporate both cybersecurity and data privacy concepts in all stages of asset and data lifecycles; and
- Document the organization's program-level guidance that defines the "who, what, why, when & how" about the organization's specific risk management practices.

SCR-RMM Step 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 SCR-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*

The SCF's Risk Catalog thirty-nine (39) risks.

SCR-RMM Step 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 cybersecurity & data 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 SCR-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:

SCR-RMM Step 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 SCF's Threat Catalog contains fourteen (14) natural threats.

SCR-RMM Step 5B. Manmade Threats

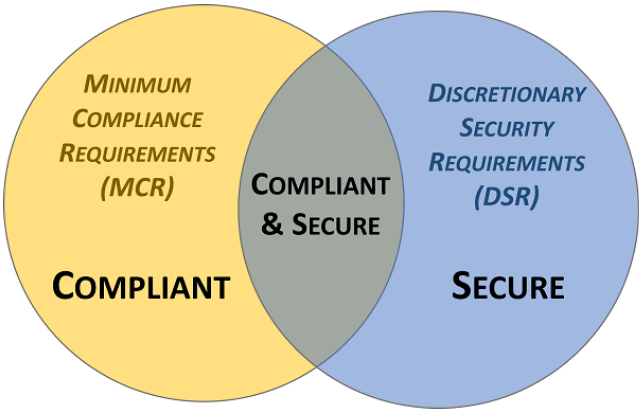
Manmade threats are caused by an element of human intent, negligence or error, or threat of violence that have the potential to impact individuals, processes, organizations or society, as a whole. The SCF's Threat Catalog contains twenty-three (23) manmade threats.

SCR-RMM Step 6. Establish A Controls Catalog

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

To assist in this process, it is helpful for the organization to categorize its applicable controls according to "must have" vs "nice to have" requirements:[42]

- Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.


Minimum Compliance Requirements (MCR)
Compliant
Compliant & Secure
Discretionary Security Requirements (DSR)
Secure

[42] *Secure, Compliant & Resilient Management System (SCRMS) model - http://integrated-controls-management.com/*

- Discretionary Security Requirements (DSR) are tied to the organization's risk appetite since DSR are "above and beyond" MCR, 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 MCR and DSR are implemented and properly governed:

- MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR 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 MCR establishes the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

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

SCR-RMM Step 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 cybersecurity and data privacy controls. This is generally defined by aligning with a Capability Maturity Model (CMM). While there are several to choose from, the SCF's Secure, Compliant & Resilient Capability Maturity Model (SCR-CMM) contains control-level criteria for each of the levels of the maturity model.

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

SCR-RMM Step 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 exist to guide the assessor when performing risk assessments.

Assessing risks in the context of the RMS applies to various assessment scenarios:

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

There are three (3) levels of rigor for a risk assessment:

1. Standard;
2. Enhanced; and
3. Comprehensive.

The definition of each assessment method includes types of objects to which the method can be applied. In addition, the application of each method is described in terms of the attributes of depth and coverage.

- The depth attribute addresses the rigor and level of detail of the assessment.
- The coverage attribute addresses the scope or breadth of the assessment.

SCR-RMM Step 8A. Risk Assessment Level 1: Standard Rigor (Minimum Assurance)

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:

1. Implemented; and
2. Free of obvious errors.

Standard rigor represents sufficient due care in the evaluation of cybersecurity and/or data protection controls. Standard rigor is appropriate for the Manual Point In Time (MPIT) assessment methodology that:

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

1. Is relevant to a specific point in time (time at which the controls were evaluated); and
2. Relies on the manual review of artifacts to derive a finding.

SCR-RMM Step 8B. Risk Assessment Level 2: Enhanced Rigor (Moderate Assurance)

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:

1. The applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors; and
2. There are increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended.

Enhanced rigor is appropriate for the Automated Point In Time (APIT) assessment methodology that utilizes automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

1. Is relevant to a specific point in time (time at which the controls were evaluated);
2. In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
3. The combined output of automated and manual reviews of artifacts is used to derive a finding.

SCR-RMM Step 8C. Risk Assessment Level 3: Comprehensive Rigor (High Assurance)

Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:

1. Whether the applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors;
2. Whether there are further increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended on an ongoing and consistent basis; and
3. There is support for continuous improvement in the effectiveness of the applicable controls.

Comprehensive rigor is appropriate for the Automated Evidence with Human Review (AEHR) assessment methodology that is used for ongoing, continuous control assessments:

1. AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
2. Recurring human reviews:
    a. Evaluate the legitimacy of the results from automated control assessments; and
    b. Validate the automated evidence review process to derive a finding.

SCR-RMM Step 9. Establish The Context For Assessing Risks

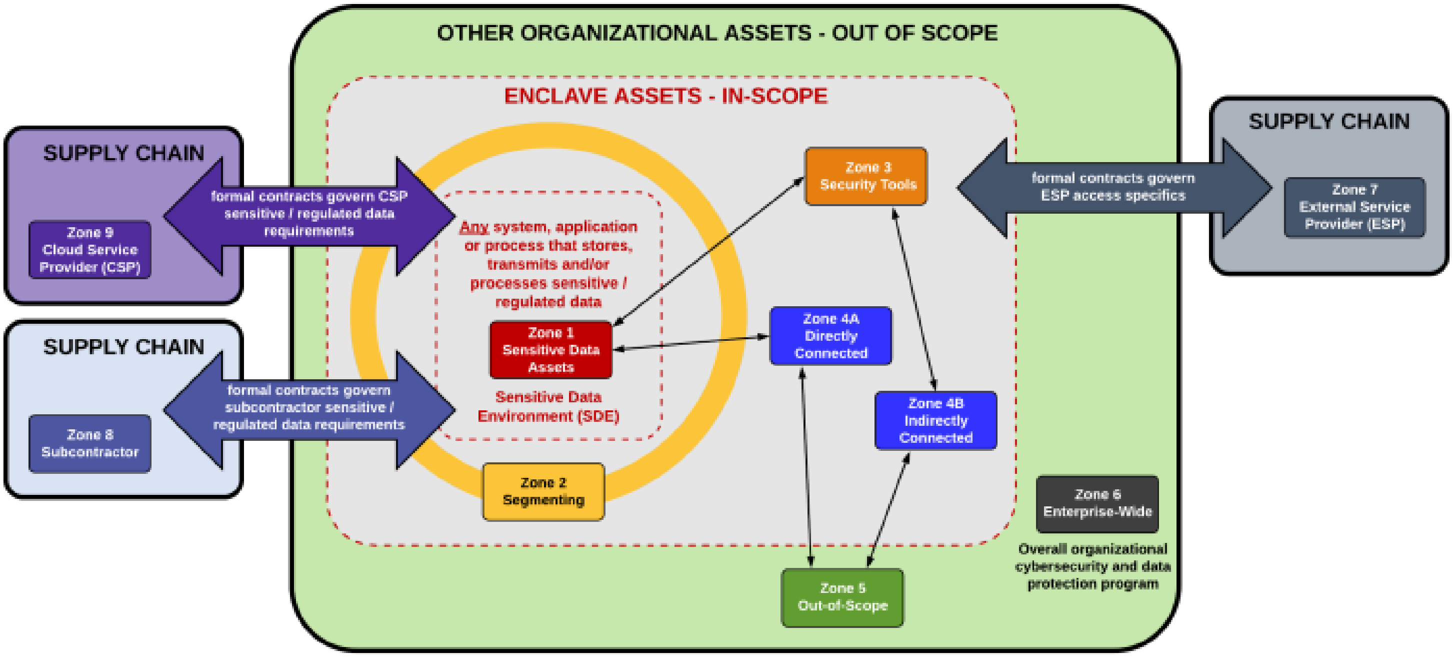
Now that a methodology exists to assess risk, it is necessary for the assessor to establish the context of the Secure, Compliant & Resilient Risk Environment (SPRE). The SPRE is the overall operating environment that is in scope for the risk assessment. This is where applicable threats, risks and vulnerabilities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

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

SPRE Context	SSPP Component
Background Information	General description & purpose
	Applicable statutory, regulatory & contractual requirements
	Applicable contracts
	Stakeholders (internal & external)
	Unique data protection considerations
System Environment Description	Hardware & software in use
	Geolocation considerations

	Identity & Access Management (**IAM**)
	Network boundaries
	Supply chain overview
	Ongoing maintenance & support plan

Without specific statutory, regulatory or contractual scoping instructions, the organization should leverage the Unified Scoping Guide (USG) as the basis for scoping sensitive and/or regulated data.[43]


OTHER ORGANIZATIONAL ASSETS - OUT OF SCOPE
ENCLAVE ASSETS - IN-SCOPE
SUPPLY CHAIN
Zone 9 Cloud Service Provider (CSP)
formal contracts govern CSP sensitive / regulated data requirements
SUPPLY CHAIN
Zone 8 Subcontractor
formal contracts govern subcontractor sensitive / regulated data requirements
Any system, application or process that stores, transmits and/or processes sensitive / regulated data
Zone 1 Sensitive Data Assets
Sensitive Data Environment (SDE)
Zone 2 Segmenting
Zone 3 Security Tools
Zone 4A Directly Connected
Zone 4B Indirectly Connected
Zone 5 Out-of-Scope
Zone 6 Enterprise-Wide
Overall organizational cybersecurity and data protection program
formal contracts govern ESP access specifics
SUPPLY CHAIN
Zone 7 External Service Provider (ESP)

SCR-RMM Step 10. Conformity Assessment (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 the organization's conformity against that specified control set.

The assessor leverages Assessment Objectives (AOs) to perform a conformity assessment against the designated cybersecurity & data protection controls. The AOs provide objective criteria that must be satisfied to legitimately determine whether the control is implemented and operating as intended.

Note: There may be multiple AOs associated with a control. The SCF spreadsheet contains an AO catalog, tied to SCF controls.

SCR-RMM Step 11. Control Assessment Methods & Findings

The process of assessing controls (including AOs) involves determining the most appropriate assessment method, the methodology that will be used to assess controls and a way to report on the resulting findings. This section covers those topics.

SCR-RMM Step 11A. Assessment Methods

Assessors are expected to review artifacts and other evidence to independently verify that an organization meets the AO for all applicable controls. There are three (3) assessment methods:

1. Examine;
2. Interview; and
3. Test.

SCR-RMM Step 11A-1. Examine

The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.

[43] *Unified Scoping Guide (USG) - https://complianceforge.com/content/pdf/unified-scoping-guide-usg.pdf*

SCR-RMM Step 11A-2. Interview

The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.

SCR-RMM Step 11A-3. Test

The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.

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

- Qualitative;
- Semi-Qualitative; or
- Quantitative

In most cases, it is not feasible to have an entirely quantitative assessment, so assessments should be expected to include semi-qualitative or qualitative aspects. There are multiple methods to actually assess and calculate risk. The SCR-RMM simplifies risk management practices by utilizing a form of risk matrix that takes Occurrence Likelihood (OL) and Impact Effect (IE) into account to determine the risk categorization.

SCR-RMM Step 11B. Methodologies

Note: There are three (3) options to implement assessment methods:

1. Manual Point In Time (MPIT);
2. Automated Point In Time (APIT); and
3. Automated Evidence with Human Review (AEHR).

SCR-RMM Step 11B-1. Manual Point In Time (MPIT)

MPIT is a traditional assessment methodology that:

- Is relevant to a specific point in time (time at which the controls were evaluated); and
- Relies on the manual review of artifacts to derive a finding;

SCR-RMM Step 11B-2. Automated Point In Time (APIT)

APIT utilizes automation to augment a traditional assessment methodology, where Artificial Intelligence and Autonomous Technologies (AAT) are used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

- Is relevant to a specific point in time (time at which the controls were evaluated);
- In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
- The combined output of automated and manual reviews of artifacts is used to derive a finding; or

SCR-RMM Step 11B-3. Automated Evidence with Human Review (AEHR)

AEHR is used for ongoing, continuous control assessments:

- AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
- Recurring human reviews:
  - Evaluate the legitimacy of the results from automated control assessments; and
  - Validate the automated evidence review process to derive a finding.

SCR-RMM Step 11C. Assessment Findings

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

The four (4) categories of findings are:

1. Satisfactory;
2. Not Applicable;
3. Compensating Control; and
4. Deficient.

SCR-RMM Step 11C-1. Satisfactory

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

SCR-RMM Step 11C-2. Not Applicable

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

SCR-RMM Step 11C-3. Compensating Control

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

SCR-RMM Step 11C-4. Deficient

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

EXPERT INSIGHT (CONTROL ASSESSMENTS): I *the context of control assessments, a designation of:*

- *Satisfactory is positive, where the assessment criteria are met;*
- *N/A is neutral, where the control, or AO, does not apply;*
- *Compensating Control is neutral, where another control, or controls, is/are designated as sufficiently reducing the risk(s) associated with the control; and*
- *Deficient is negative, where the assessment criteria are not met;*

SCR-RMM Step 12. Determine Risk Exposure

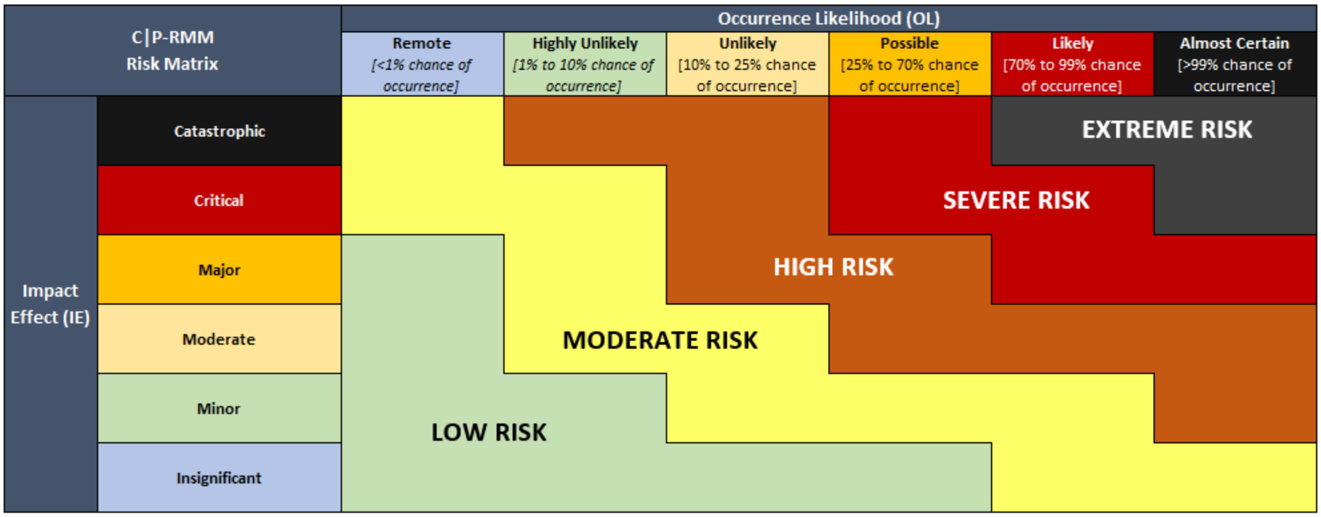
Based on deficient controls identified in the previous step, it is necessary to determine the organization's exposure to risk, since the control deficiency(ies) creates risk (e.g., a situation where someone or something valued is exposed to danger, harm or loss).

The SCR-RMM leverages the following five (5) categories of risk:

1. Low;
2. Moderate;
3. High;
4. Severe; and
5. Extreme.

These categories of risk are determined through an intersection of:

1. Impact Effect (IE); and
2. Occurrence Likelihood (OL)


C|P-RMM
Risk Matrix
Occurrence Likelihood (OL)
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]
Impact Effect (IE)
Catastrophic
Critical
Major
Moderate
Minor
Insignificant
EXTREME RISK
SEVERE RISK
HIGH RISK
MODERATE RISK
LOW RISK

SCR-RMM Step 12A. Impact Effect (IE)

The six (6) categories of IE are:

1. Insignificant *(e.g., organization-defined little-to-no impact to business operations);*
2. Minor *(e.g., organization-defined minor impacts to business operations)*;
3. Moderate *(e.g., organization-defined moderate impacts to business operations)*;
4. Major *(e.g., organization-defined major impacts to business operations)*;
5. Critical *(e.g., organization-defined critical impacts to business operations)*; and
6. Catastrophic *(e.g., organization-defined catastrophic impacts to business operations).*

SCR-RMM Step 12B. Occurrence Likelihood (OL)

The six (6) categories of OL are:

1. Remote possibility *(e.g., <1% chance of occurrence)*;
2. Highly unlikely *(e.g., from 1% to 10% chance of occurrence)*;
3. Unlikely *(e.g., from 10% to 25% chance of occurrence)*;
4. Possible *(e.g., from 25% to 70% chance of occurrence)*;
5. Likely *(e.g., from 70% to 99% chance of occurrence)*; and
6. Almost certain *(e.g., >99% chance of occurrence)*.

There are three (3) general approaches are commonly employed to estimate OL:

1. Relevant historical data;
2. Probability forecasts; and
3. Expert opinion.

SCR-RMM Step 12C. Inherent Risk

From the risk assessment matrix, the intersection between OL and IE will provide the inherent ris" 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.

SCR-RMM Step 12D. Residual Risk

Residual risk takes into account control weighting, the maturity of implemented controls and other mitigating factors where it builds upon the inherent risk calculation. To identify the residual risk score, OL is calculated by IE, Control Weighting (CW), Maturity Level (ML) and Mitigating Factors (MF).

SCR-RMM Step 13. Prioritize & Document Identified Deficiencies

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

- Emergency;
- Elevated; or
- Standard.

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

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

SCR-RMM Step 14. Risk Determination: Report on Conformity (ROC)

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

This approach can be summarized by reporting to the organization's management on the "health" of the assessed controls by one of the following four (4) risk determinations:

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

1. Strictly Conforms;
2. Conforms;
3. Significant Deficiency; and
4. Material Weakness.

SCR-RMM Step 14A. Strictly Conforms

This is a positive outcome and indicates that at a high-level, the organization's cybersecurity and data privacy practices conform to its selected cybersecurity and data privacy practices. Strictly Conforms means:

- The organization/LOB can demonstrate Strict Conformity with its selected cybersecurity and/or data protection controls, where one hundred percent (100%) of the assessed controls have reasonable evidence to conclude:
  - The controls are met and operational;
  - Any control designated as Not Applicable (N/A) is validated as such by the assessor; and/or
  - Where applicable, compensating controls are validated by the assessor as being:
    - Applicable;
    - Reasonable; and
    - Implemented and operating properly; and
- Assessed controls provide reasonable assurance that the organization's/LOB's cybersecurity and data protection program provides adequate security, where it:
  - Adheres to a defined and documented risk tolerance;
  - Mitigates material cybersecurity and/or data protection risks;
  - Is designed to detect and protect against material cybersecurity and/or data protection threats; and
  - Is prepared to respond to material incidents.

Strictly Conforms is a statement to the organization's management that sufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance can be achieved.

SCR-RMM Step 14B. Conforms

This is a positive outcome and indicates that at a high-level, the organization's cybersecurity and data privacy practices conform to its selected cybersecurity and data privacy practices. Conforms means:

- The organization/LOB can demonstrate Conformity with its selected cybersecurity and/or data protection controls, where at least eighty percent (80%) of the assessed controls have reasonable evidence to conclude:
  - The controls are met and operational;
  - Any control designated as Not Applicable (N/A) is validated as such by the assessor; and/or
  - Where applicable, compensating controls are validated by the assessor as being:
    - Applicable;
    - Reasonable; and
    - Implemented and operating properly; and
- Any assessed control deficiency is not material to the organization's/LOB's cybersecurity and data protection program; and
- Assessed controls provide reasonable assurance that the organization's/LOB's cybersecurity and data protection program provides adequate security, where it:
  - Adheres to a defined and documented risk tolerance;
  - Mitigates material cybersecurity and/or data protection risks;
  - Is designed to detect and protect against material cybersecurity and/or data protection threats; and
  - Is prepared to respond to material incidents.

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

SCR-RMM Step 14C. Significant Deficiency

This is a negative outcome and indicates the organization was unable to demonstrate conformity with its selected cybersecurity and data privacy practices, due to systematic problems. Significant Deficiency means:

- The organization/LOB can demonstrate limited conformity with its selected cybersecurity and/or data protection controls due to a systemic problem within the organization's cybersecurity and data protection program, where:
  - At least seventy percent (70%), but less than eighty percent (80%), of the assessed controls have reasonable evidence to conclude:
    - The controls are met and operational;

        - Any control designated as N/A is validated as such by the assessor; and/or
        - Where applicable, compensating controls are validated by the assessor as being:
            - Applicable;
            - Reasonable; and
            - Implemented and operating properly;
- Any assessed control deficiency is not material to the organization's cybersecurity and data protection program;
- Assessed controls do not provide reasonable assurance that the organization's cybersecurity and data protection program provides adequate security, where it:
    - Adheres to a defined and documented risk tolerance;
    - Mitigates material cybersecurity and/or data protection risks;
    - Is designed to detect and protect against material cybersecurity and/or data protection threats; and
    - Is prepared to respond to material incidents; and
- The organization's cybersecurity and data protection program:
    - Has systemic problems inherent in the overall function of a team, department, project, application, service and/or vendor rather than a specific, isolated factor; and
    - Requires implementing limited changes to personnel, technology and/or practices to correct the design and implementation of deficient cybersecurity and/or data protection controls.

Significant Deficiency is a statement to the organization's management that insufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance is achieved, due to a systemic problem in the cybersecurity and/or privacy program.

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

SCR-RMM Step 14D. Material Weakness

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

- The organization/LOB cannot demonstrate conformity with its selected cybersecurity and/or data protection controls due to deficiencies that make it probable that reasonably expected threats will not be promptly detected or prevented, where:
    - One (1), or more, material controls is/are deficient; and/or
    - Less than seventy percent (70%) of the assessed controls have reasonable evidence to conclude:
        - The controls are met and operational;
        - Any control designated as N/A is validated by the assessor and confirmed as such; and/or
        - Where applicable, compensating controls are validated by the assessor as being:
            - Applicable;
            - Reasonable; and
            - Implemented and operating properly;
- Assessed controls do not provide reasonable assurance that the organization's cybersecurity and data protection program adequately:
    - Adheres to a defined and documented risk tolerance;
    - Mitigates material cybersecurity and/or data protection risks; and/or
    - Possesses the capability to:
        - Detect and protect against material cybersecurity and/or data protection threats; and/or
        - Respond to material incidents; and
- The organization's cybersecurity and data protection program:
    - Cannot perform its stated mission; and
    - Drastic changes to people, processes and/or technologies are required to remediate the deficiencies.

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

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

SCR-RMM Step 15. Identify The Appropriate Management Audience

It is critically important that as part of an entity's program to manage risk that various levels of management are identified with varying authority, each with a pre-described ability to make risk management decisions. This helps prevent low-level managers from recklessly accepting risks that should be reserved for more senior management. A common tiered structure for risk management decisions includes:

- Line Management;
- Senior Management;
- Executive Management; and
- Board of Directors.

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

SCR-RMM Step 16. Management Determines Risk Treatment

Risk management is a management decision:

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

Common risk treatment options include:

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

SCR-RMM Step 17. Cybersecurity & Data Protection Practitioners Implement & Document Risk Treatment

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

- Open (unacceptable risk);
- Open (acceptable risk); and
- Closed.

Calculating Risk: Inherent Risk vs Residual Risk

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

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

SCR-RMM Calculations Step 1: Calculate The Inherent Risk

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

SCR-RMM Calculations Step 2: Account For Control Weighting

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

SCR-RMM Calculations Step 3: Account For Maturity Level Targets

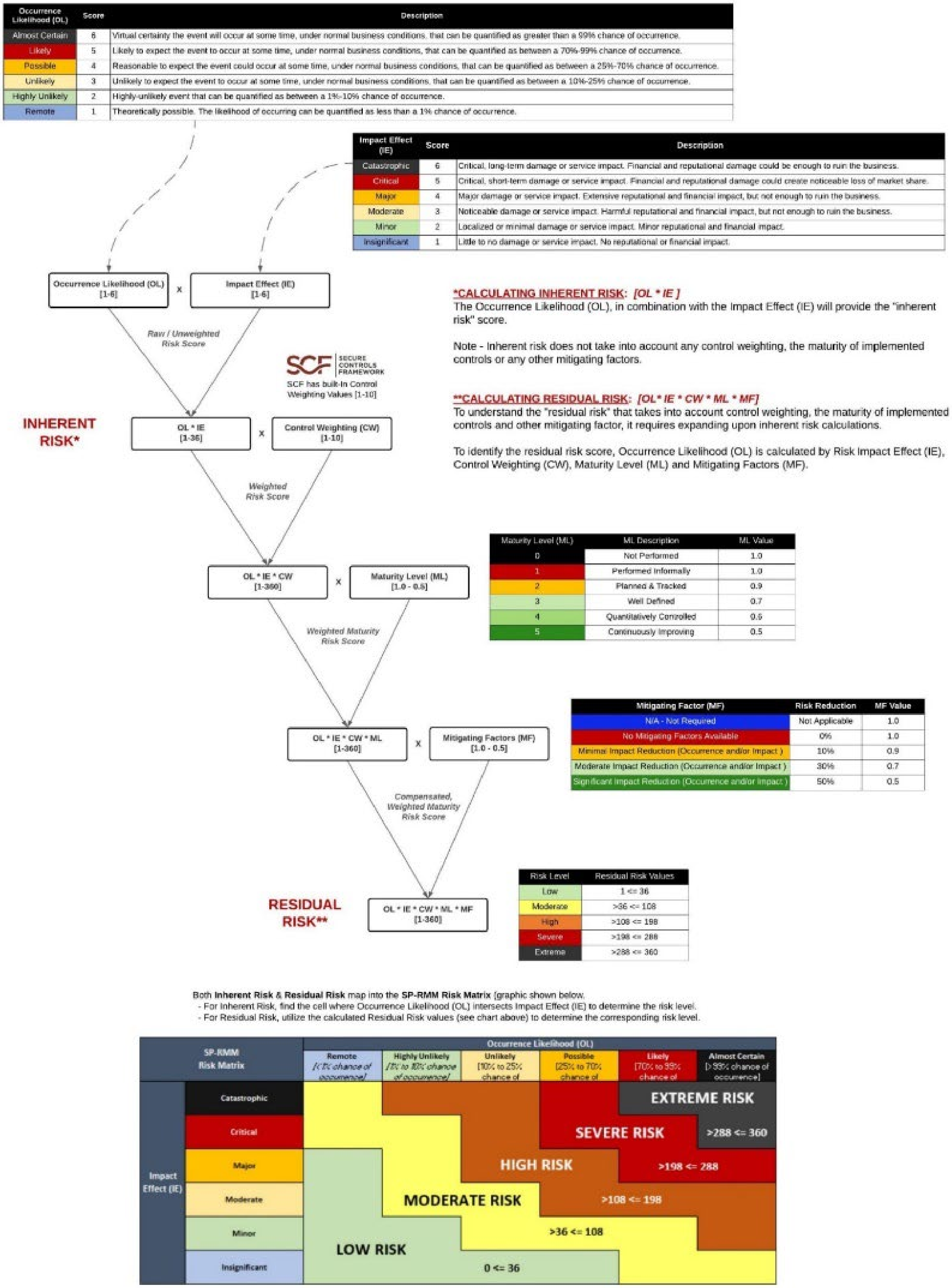
The next step is meant to determine a weighted maturity score that takes control maturity into account. The more mature a control is, the greater the risk should be reduced. Maturity Level (ML) is multiplied by the value determined in Step 2.

SCR-RMM Calculations Step 4: Account For Mitigating Factors To Determine Residual Risk

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

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

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.



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

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

Occurrence Likelihood (OL) [1-6]
x
Impact Effect (IE) [1-6]
Raw / Unweighted Risk Score
SCF SECURE CONTROLS FRAMEWORK
SCF has built-in Control Weighting Values [1-10]
INHERENT RISK*
OL * IE [1-36]
x
Control Weighting (CW) [1-10]
Weighted Risk Score
OL * IE * CW [1-360]
x
Maturity Level (ML) [1.0 - 0.5]
Weighted Maturity Risk Score
OL * IE * CW * ML [1-360]
x
Mitigating Factors (MF) [1.0 - 0.5]
Compensated, Weighted Maturity Risk Score
RESIDUAL RISK**
OL * IE * CW * ML * MF [1-360]

***CALCULATING INHERENT RISK:** *[OL * IE]*
The Occurrence Likelihood (OL), in combination with the Impact Effect (IE) will provide the "inherent risk" score.

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

****CALCULATING RESIDUAL RISK:** *[OL* IE * CW * ML * MF]*
To understand the "residual risk" that takes into account control weighting, the maturity of implemented controls and other mitigating factor, it requires expanding upon inherent risk calculations.

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

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

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

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

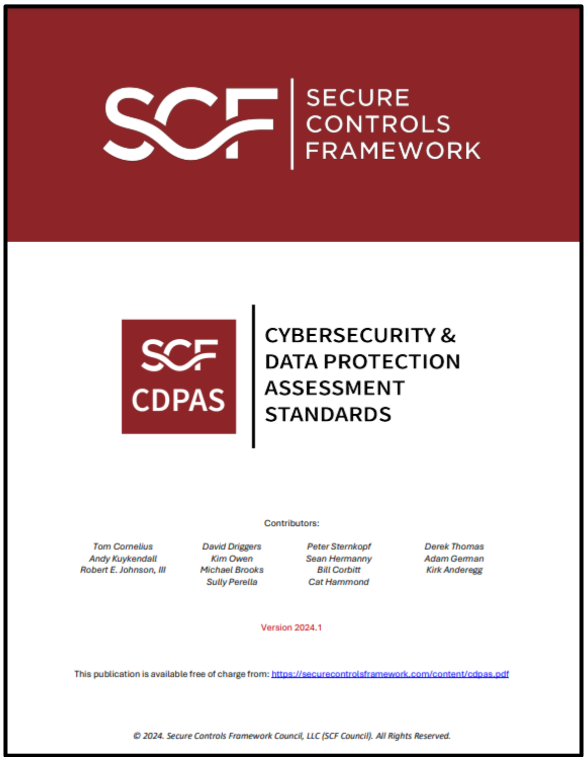
Both **Inherent Risk & Residual Risk** map into the **SP-RMM Risk Matrix** (graphic shown below.
- For Inherent Risk, find the cell where Occurrence Likelihood (OL) intersects Impact Effect (IE) to determine the risk level.
- For Residual Risk, utilize the calculated Residual Risk values (see chart above)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

SP-RMM Risk Matrix
Occurrence Likelihood (OL)
Remote [<1% chance of occurrence]
Highly Unlikely [1% to 10% chance of occurrence]
Unlikely [10% to 25% chance of
Possible [25% to 70% chance of
Likely [70% to 99% chance of
Almost Certain [>99% chance of occurrence]
Impact Effect (IE)
Catastrophic
Critical
Major
Moderate
Minor
Insignificant
EXTREME RISK
>288 <= 360
SEVERE RISK
>198 <= 288
HIGH RISK
>108 <= 198
MODERATE RISK
>36 <= 108
LOW RISK
0 <= 36

[graphic download - https://securecontrolsframework.com/content/SCF-Risk-Management-Model-Calculations.pdf]

SECTION 11. SCF CYBERSECURITY & DATA PROTECTION ASSESSMENT STANDARDS (CDPAS)

The Cybersecurity & Data Protection Assessment Standards (CDPAS) is a cohesive, consistent set of standards for performing cybersecurity and data protection-related Third Party Assessment, Attestation and Certification Services (3PAAC Services). [44] By following the Cybersecurity & Data Protection Assessment Standards (CDPAS) approach, cybersecurity and data protection practitioners can improve the currently disjointed approach used to perform assessments of cybersecurity and/or data protection controls. The CDPAS is a "standard" that normalizes third-party assessment practices.



SECURE CONTROLS FRAMEWORK

SCF CDPAS

CYBERSECURITY & DATA PROTECTION ASSESSMENT STANDARDS

Contributors:

Tom Cornelius
Andy Kuykendall
Robert E. Johnson, III

David Driggers
Kim Owen
Michael Brooks
Sully Perella

Peter Sternkopf
Sean Hermanny
Bill Corbitt
Cat Hammond

Derek Thomas
Adam German
Kirk Anderegg

Version 2024.1

This publication is available free of charge from: https://securecontrolsframework.com/content/cdpas.pdf

© 2024. Secure Controls Framework Council, LLC (SCF Council). All Rights Reserved.

[CDPAS download – https://securecontrolsframework.com/content/cdpas.pdf]

CDPAS PURPOSE

The CDPAS exists to provide performance standards for cybersecurity and data protection-related 3PAAC Services.

CDPAS INTENT

The CDPAS is not "one-size-fits-all." Instead, the guidance throughout this document should be adopted and tailored to the unique size, resources and risk circumstances of each OSA and 3PAO. The CDPAS can be modified, or augmented, with OSA-specific requirements, policies, or other compliance obligations due to statutory, regulatory and/or contractual requirements. This publication empowers OSAs to develop cybersecurity and data protection assessment strategies tailored to their specific mission, business needs, threats and operational environments.

CDPAS STANDARDS

The following are the names of each CDPAS standard. The associate standard, justification and guidance can be found in the CDPAS document: [45]

1. Professional Duty of Care
    1.1. Ethical Conduct
    1.2. Independence
    1.3. Subject Matter Competency
    1.4. Conflict of Interest (COI) Avoidance
2. Secure Practices

[44] *SCF CDPAS - https://securecontrolsframework.com/content/cdpas.pdf*

[45] *SCF CDPAS - https://securecontrolsframework.com/content/cdpas.pdf*

- 2.1. Security & Privacy By Design
- 2.2. Statement of Work (SOW)
- 2.3. Assessment-Specific Data Protection Impact Assessment (DPIA)
- 2.4. Intellectual Property (IP) Protections
- 2.5. Protection of Assessment Information
- 2.6. Use of Assessment Information
- 2.7. Disposal of Assessment Information

3. Due Diligence
   - 3.1. Adherence To Data Protection CDPAS Requirements
   - 3.2. Assessment Boundary Demarcation
   - 3.3. Graphical Representation of Assessment Boundary
   - 3.4. Stakeholder Identification
   - 3.5. Control Reciprocity
   - 3.6. Control Inheritance
   - 3.7. Defined Cybersecurity and/or Data Privacy Controls
   - 3.8. Defined Risk Tolerance
   - 3.9. Defined Maturity Level
   - 3.10. Defined Materiality Threshold
   - 3.11. Material Risk Designation
   - 3.12. Material Threat Designation
   - 3.13. Material Incident Designation
   - 3.14. Internal Assessment
4. Due Diligence – Assessors & 3PAOs
   - 4.1. Formalized Assessment Plan
   - 4.2. Defined Assessment Boundaries
   - 4.3. Validate Control Applicability
   - 4.4. Defined Evidence Request List (ERL)
   - 4.5. Explicit Authorization For Testing
   - 4.6. First-Party Declarations (1PD) - Control Inheritance
   - 4.7. Third-Party Attestations (3PA) - Control Inheritance & Reciprocity
   - 4.8. Stakeholder Validation
5. Due Care - OSAs
   - 5.1. Proactive Governance
   - 5.2. Non-Conformity Oversight
   - 5.3. Annual Affirmation
6. Due Care – Assessors & 3PAOs
   - 6.1. Assessment Methods
   - 6.2. Assessment Rigor
   - 6.3. Assessing Based On Control CDPAS Applicability
   - 6.4. Assessment Objectives (AOs)
   - 6.5. Control Designation
   - 6.6. Objectivity Through Reasonable Interpretation
   - 6.7. Adequate Sampling
   - 6.8. Assessment Tools & Automation
7. Quality Control
   - 7.1. Assessment Findings
   - 7.2. Objective Peer Review
8. Conformity Designation
   - 8.1. Report On Conformity (ROC)
   - 8.2. Assessment Finding Challenges
9. Maintaing Conformity
   - 9.1. Plan of Action & Milestones (POA&M)
   - 9.2. Changes Affecting The Assessment Boundary
   - 9.3. Reassessments Due To Material Change

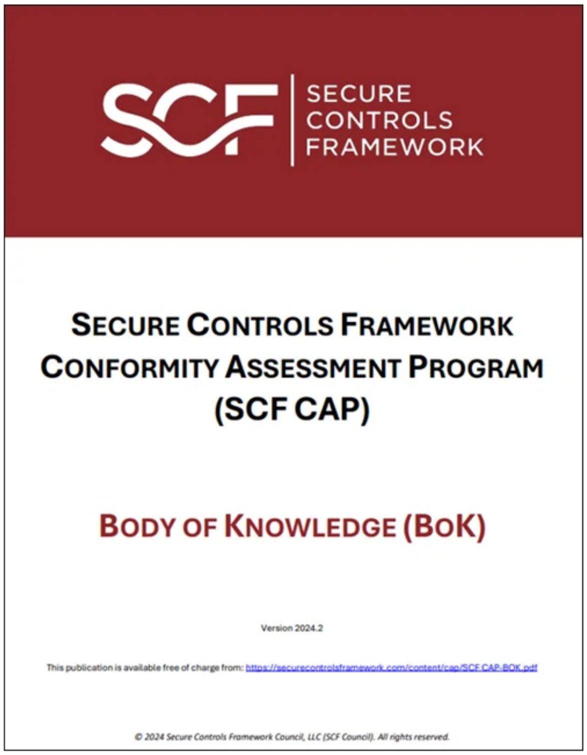
Section 12. Secure Controls Framework Conformity Assessment Program (SCF CAP)

The SCF Conformity Assessment Program (SCF CAP) is an organization-level conformity assessment. The SCF CAP is designed to utilize tailored cybersecurity and data privacy controls that specifically address the applicable statutory, regulatory and contractual obligations an Organization Seeking Assessment (OSA) is required to comply with. By using the metaframework nature of the SCF, an OSA is able to perform conformity assessment that spans multiple cybersecurity and data privacy-specific laws, regulations and frameworks.

The SCF CAP is focused on using the SCF as the control set to provide a company-level certification. While the SCF-CAP shares some similarities with other existing, single-focused certifications (e.g., ISO 27001, CMMC, FedRAMP, etc.), the SCF CAP is unique in its metaframework approach to covering cybersecurity and data protection requirements that span multiple laws, regulations and frameworks

SCF CAP Body of Knowledge (SCF CAP BoK)

The gain an understanding of what the SCF CAP is and how to get SCF certified, start with the SCF CAP Body of Knowledge (SCF CAP BoK), since it is the authoritative source for the SCF CAP.[46]



SECURE CONTROLS FRAMEWORK

SECURE CONTROLS FRAMEWORK CONFORMITY ASSESSMENT PROGRAM (SCF CAP)

BODY OF KNOWLEDGE (BOK)

Version 2024.2

This publication is available free of charge from: https://securecontrolsframework.com/content/cap/SCF-CAP-BOK.pdf

© 2024 Secure Controls Framework Council, LLC (SCF Council). All rights reserved.

[SCF CAP BoK download - https://securecontrolsframework.com/content/cap/scf-cap-bok.pdf]

ABC's of Conformity Assessment

NIST Special Publication 200-01, *ABC's of Conformity Assessment*, is where you should start to understand what a conformity assessment is and why it is important.[47] That document is designed to provide the reader with an introduction to conformity assessment and information on how the various conformity assessment activities are interlinked.

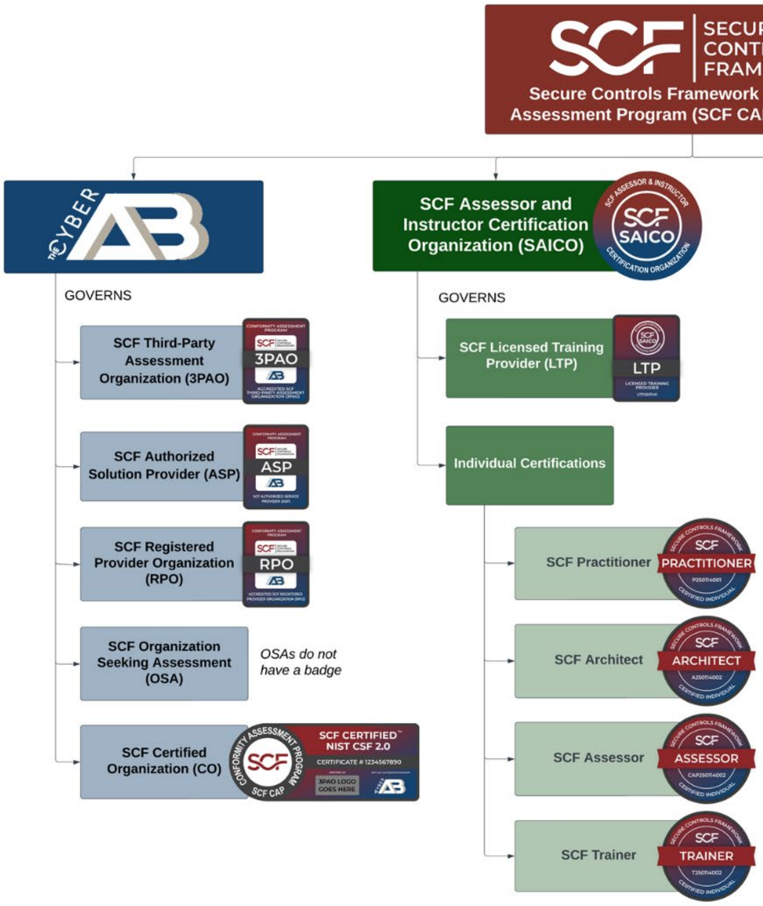
[46] *SCF CAP BoK - https://securecontrolsframework.com/content/cap/scf-cap-bok.pdf*

[47] *NIST SP 2000-01 - NIST Special Publication 200-01, ABC's of Conformity Assessment*

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

SCF CAP Ecosystem

The SCF CAP Ecosystem consists of several entities and multiple independent parties:


SCF SECURE CONTROLS FRAMEWORK
Secure Controls Framework Conformity Assessment Program (SCF CAP) Ecosystem
THE CYBER AB
SCF Assessor and Instructor Certification Organization (SAICO)
SCF CONNECT
SCF Licensed Content Provider (LCP)
LCP
LICENSED CONTENT PROVIDER (LCP)
GOVERNS
GOVERNS
GOVERNS
SCF LICENSED 3RD PARTY CONTENT
SCF Third-Party Assessment Organization (3PAO)
3PAO
SCF Authorized Solution Provider (ASP)
ASP
SCF Registered Provider Organization (RPO)
RPO
SCF Organization Seeking Assessment (OSA)
OSAs do not have a badge
SCF Certified Organization (CO)
CONFORMITY ASSESSMENT PROGRAM
SCF CAP
SCF CERTIFIED™ NIST CSF 2.0
CERTIFICATE # 1234567890
3PAO LOGO GOES HERE
SCF Licensed Training Provider (LTP)
LTP
Individual Certifications
SCF Practitioner
PRACTITIONER
SCF Architect
ARCHITECT
SCF Assessor
ASSESSOR
SCF Trainer
TRAINER
SCF Authorized Control Integrator (ACI)
ACI

The Cyber AB

The Cyber AB governs the following aspects of the SCF CAP Ecosystem:

- **SCF Third-Party Assessment Organization (SCF 3PAO).** SCF 3PAOs are entities accredited by The Cyber AB to conduct SCF-related Third-Party Assessment, Attestation, and Certification (3PAAC) services for Organizations Seeking Assessment (OSA) under the SCF CAP. These organizations provide objective, consistent, thorough, and reliable assessments of an OSA's implementation of the SCF, ensuring conformance with specified cybersecurity and/or data protection requirements. SCF 3PAOs play a critical role in maintaining the integrity and credibility of SCF certifications through rigorous and impartial assessments.
- **SCF Authorized Solutions Provider (SCF ASP).** SCF ASPs are cloud-based platforms, including Cloud Service Providers (CSPs), Managed Service Providers (MSPs), Managed Security Service Providers (MSSP), and other platform- or process-oriented service providers that operate within the defined scope of the SCF framework. SCF ASPs provide a structured platform environment for implementing SCF principles within cloud infrastructures and related technological solutions, reinforcing the integrity and effectiveness of SCF-compliant operations.
- **SCF Registered Provider Organization (SCF RPO).** SCF RPOs are organizations that provide SCF-related professional services, including consulting and implementation. SCF RPOs assist organizations in preparing for assessments, streamlining SCF adoption, and ensuring alignment with cybersecurity and compliance objectives. SCF RPOs have demonstrated a commitment to professionalism and expertise in implementing the SCF within diverse business environments.
- **SCF Organizations Seeking Assessment (SCF OSA).** SCF OSAs are organizations that are working towards earning a SCF-based certification, but have not yet undergone a SCF CAP conformity assessment.
- **SCF Certified Organization (SCF CO).** SCF COs are SCF OSA that have successfully passed an SCF CAP conformity assessment and have earned an SCF Certified designation. These organizations have demonstrated conformity with the SCF, establishing the SCF CO as a trusted and compliant entity within the SCF CAP Ecosystem. SCF COs maintain their certification through ongoing compliance efforts, periodic assessments, and adherence to SCF standards.

SCF Assessor and Instructor Certification Organization (SAICO)

SCF Assessor and Instructor Certification Organization (SAICO) governs the following aspects of the SCF CAP Ecosystem:

- **SCF Practitioner.** SCF Practitioners are SAICO-certified individuals who have the knowledge and skills to (1) Implement SCF controls that align with the SCF recommended practices and structure; and (2) Maintain an organization's cybersecurity and data protection program.
- **SCF Architect.** SCF Architects are SAICO-certified individuals who have advanced SCF-related knowledge and competence necessary to (1) Architect and design SCF-based cybersecurity and data protection programs that are capable of addressing the tactical, operational and strategic needs of the organization specific to its unique People, Processes, Technologies, Data and Facilities (PPTDF) considerations; (2) Assist SCF Practitioners with the implementation of SCF controls; and (3) Make adjustments to the cybersecurity and data protection programs to account for new and/or changed laws, regulations and frameworks that affect the PPTDF.
- **SCF Assessor.** SCF Assessors are SAICO-certified individuals who are (1) Qualified to participate in and/or lead a SCF Third-Party Assessment Organization's (3PAO's) assessment team to perform SCF Conformity Assessment Program (SCF CAP) assessments; and (2) Knowledgeable to analyze SCF controls to determine if the control is appropriate, properly implemented and produces the desired results to meet Assessment Objectives (AOs).
- **SCF Licensed Training Provider (SCF LTP).** SCF LTPs are SAICO-certified organizations that deliver a SAICO-approved individual-level certification training program using SCF Trainers.
- **SCF Trainer.** SCF Trainers are SAICO-certified individuals responsible for delivering initial and recurring SCF-based educational training for SAICO-approved individual-level certifications.

SCF Connect

SCF Connect governs the following aspects of the SCF CAP Ecosystem:

- **Single Source of Truth (SSOT).** SCF Connect is a Governance, Risk & Compliance (GRC) platform that is designated to be the SSOT for SCF-related 3PAAC activities. OSAs will be provided with an account on SCF Connect to prepare for and conduct its SCF CAP conformity assessment. SCF Connect is a SCF ACI.
- **SCF Authorized Controls Integrator (SCF ACI).** SCF ACIs are Governance, Risk, and Compliance (GRC) platforms that specialize in integrating the SCF framework. SCF ACIs facilitate seamless integration, accurate compliance interpretation, and structured risk management to ensure GRC tools effectively operationalize SCF compliance. By embedding SCF CAP best practices into data, risk, and compliance management workflows, SCF ACIs reinforce a structured and scalable approach to SCF implementation within GRC environments, enhancing organizations' ability to manage risk and ensure cross-regulatory compliance effectively.

The SCF Council

The SCF Council governs the following aspects of the SCF CAP Ecosystem:

- **SCF CAP Body of Knowledge (SCF CAP BoK).** SCF CAP BoK describes SCF-related 3PAAC activities.
- **SCF CAP Assessment Guides.** SCF Assessment Guides provides Law, Regulation & Framework (LRF)-specific conformity assessment guidance for conducting SCF-related 3PAAC activities.
- **SCF Licensed Content Provider (SCF LCP).** SCF LCPs are entities authorized by SCF Council to create derivative content of the SCF, such as SCF-based policies, standards, procedures, etc. SCF LCPs play a critical role in ensuring quality control for documentation to help operationalize the SCF according to leading practices.

Section 13. Risk & Threat Catalogs

The SCF contains both a risk and threat catalog as part of the Excel download.

SCF Risk Catalog

The use case for the SCF's 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*?). A "risk" is defined as:

Noun: A situation where someone or something valued is exposed to danger, harm or loss.
Verb: To expose someone or something valued to danger, harm or loss.

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

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

With this understanding of what risk is, the SCF contains a catalog of thirty-nine (39) risks:

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

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

	R-BC-3	Reduction in productivity	Diminished user productivity.
	R-BC-4	Information loss / corruption or system compromise due to technical attack	A technical attack that compromises data, systems, applications or services (e.g., malware, phishing, hacking, etc.).
	R-BC-5	Information loss / corruption or system compromise due to non-technical attack	A non-technical attack that compromises data, systems, applications or services (e.g., social engineering, sabotage, etc.).
Exposure	R-EX-1	Loss of revenue	A negative impact on the ability to generate revenue (e.g., a loss of clients or an inability to generate future revenue).
	R-EX-2	Cancelled contract	A cancelled contract with a client or other entity for cause (e.g., failure to fulfill obligations for secure practices).
	R-EX-3	Diminished competitive advantage	Diminished competitive advantage (e.g., lose market share, internal dysfunction, etc.).
	R-EX-4	Diminished reputation	Diminished brand value (e.g., tarnished reputation).
	R-EX-5	Fines and judgements	Financial damages due to fines and/or judgements from statutory / regulatory / contractual non-compliance.
	R-EX-6	Unmitigated vulnerabilities	Unmitigated technical vulnerabilities that lack compensating controls or other mitigation actions.
	R-EX-7	System compromise	A compromise of a system, application or service that affects confidentiality, integrity, availability and/or safety.
Governance	R-GV-1	Inability to support business processes	Insufficient cybersecurity and/or privacy practices that cannot securely support the organization's technologies & processes.
	R-GV-2	Incorrect controls scoping	Missing or incorrect cybersecurity and/or privacy controls due to incorrect or inadequate control scoping practices.
	R-GV-3	Lack of roles & responsibilities	Insufficient cybersecurity and/or privacy roles & responsibilities that cannot securely support the organization's technologies & processes.
	R-GV-4	Inadequate internal practices	Insufficient cybersecurity and/or privacy practices that can securely support the organization's technologies & processes.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

	R-GV-5	Inadequate third-party practices	Insufficient Cybersecurity Supply Chain Risk Management (C-SCRM) practices that cannot securely support the organization's technologies & processes.
	R-GV-6	Lack of oversight of internal controls	The inability to demonstrate appropriate evidence of due diligence and due care in overseeing the organization's internal cybersecurity and/or privacy controls.
	R-GV-7	Lack of oversight of third-party controls	The inability to demonstrate appropriate evidence of due diligence and due care in overseeing third-party cybersecurity and/or privacy controls.
	R-GV-8	Illegal content or abusive action	Disruptive content or actions that negatively affect business operations (e.g., abusive content, harmful speech, threats of violence, illegal content, etc.).
Incident Response	R-IR-1	Inability to investigate / prosecute incidents	Insufficient incident response practices that prevent the organization from investigating and/or prosecuting incidents (e.g., chain of custody corruption, available sources of evidence, etc.).
	R-IR-2	Improper response to incidents	The inability to appropriately respond to incidents in a timely manner.
	R-IR-3	Ineffective remediation actions	The inability to ensure incident response actions were correct and/or effective.
	R-IR-4	Expense associated with managing a loss event	Financial repercussions from responding to an incident or loss.
Situational Awareness	R-SA-1	Inability to maintain situational awareness	The inability to detect cybersecurity and/or privacy incidents (e.g., a lack of situational awareness).
	R-SA-2	Lack of a security-minded workforce	The inability to appropriately educate and train personnel to foster a security-minded workforce.
Supply Chain	R-SC-1	Third-party cybersecurity exposure	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from third-party cybersecurity practices, vulnerabilities and/or incidents that affects the supply chain through impacted products and/or services.
	R-SC-2	Third-party physical security exposure	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from physical security exposure of third-party structures, facilities and/or other physical assets that affects the supply chain through impacted products and/or services.
	R-SC-3	Third-party supply chain relationships, visibility and controls	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from "downstream" third-party relationships, visibility and controls that affect the supply chain through impacted products and/or services.
	R-SC-4	Third-party compliance / legal exposure	The inability to maintain compliance due to third-party non-compliance, criminal acts, or other relevant legal action(s).

	R-SC-5	Use of product / service	The misuse of the product / service in a manner that it was not designed or how it was approved for use.
	R-SC-6	Reliance on the third-party	The inability to continue business operations, due to the reliance on the third-party product and/or service.

SCF Threat Catalog

It is necessary to develop a threat catalog that identifies possible natural and man-made threats that affect the entity's cybersecurity & data 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 SCR-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:

Natural Threats

Natural threats are caused by environmental phenomena that have the potential to impact individuals, processes, organizations or society, as a whole. The SCF's Threat Catalog contains 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.

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 SCF's Threat Catalog contains twenty-three (23) 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

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

		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 of 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 business. 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 to (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 (including loss of life).
MT-11	Statutory / Regulatory / Contractual Obligation	Laws, regulations and/or contractual obligations that directly or indirectly weaken an organization's security & privacy controls. This includes hostile nation states that leverage statutory and/or regulatory means for economic or political espionage and/or cyberwarfare activities.
MT-12	Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) Data	Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data is information an organization utilizes for business processes even though the data is untrustworthy, due to the data's currency, accuracy, integrity and/or applicability.
MT-13	Artificial Intelligence & Autonomous Technologies (AAT)	Artificial Intelligence & Autonomous Technologies (AAT) is a broad category that ranges from non-malicious failure due to a defect in the algorithm to emergent properties or unintended consequences. AAT failures can be due to hardware failures, inherent biases or other flaws in the underlying algorithm. These incidents

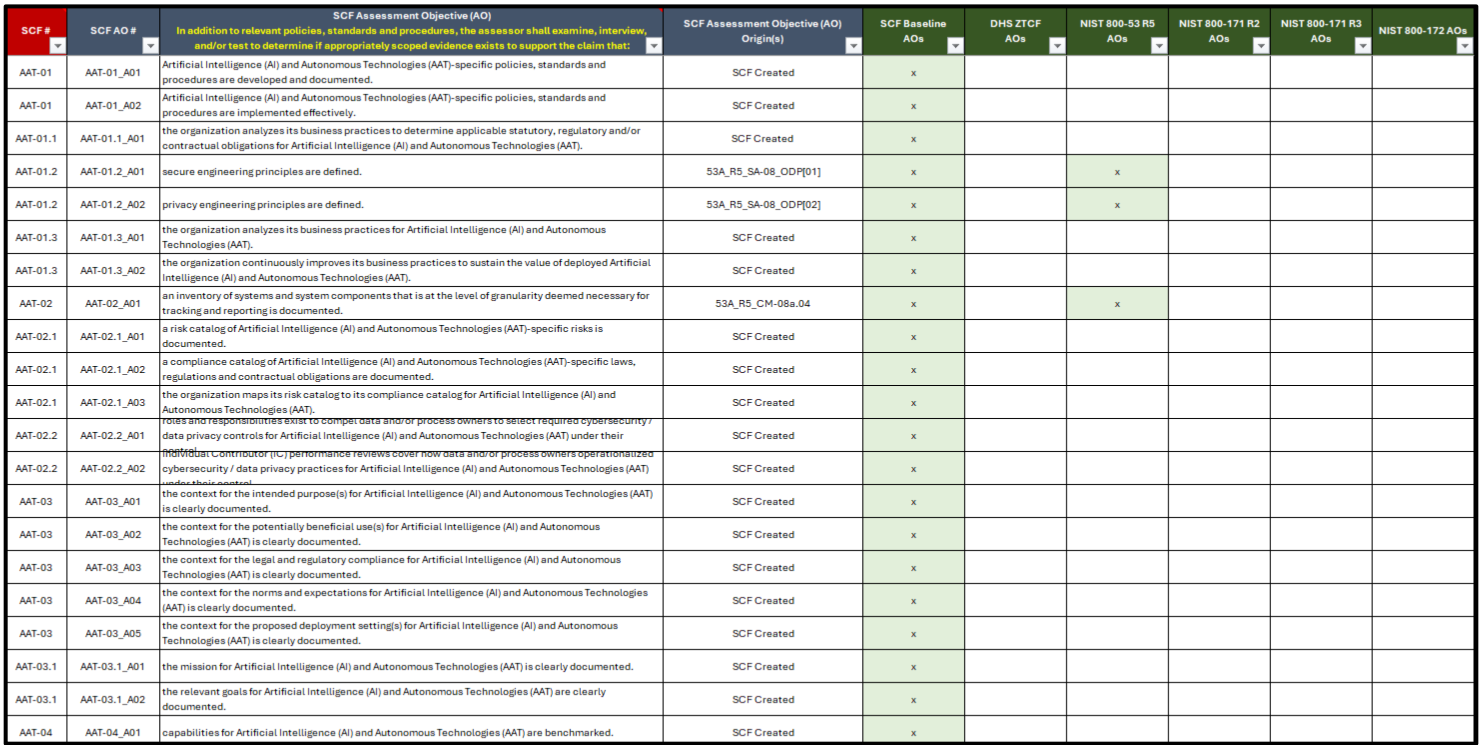
This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

		can range from malfunctions, to reliability concerns to catastrophic damage (including loss of life).
MT-14	Fraud, Corruption and/or Willful Criminal Conduct	Willful criminal conduct is a broad category that includes consciously-committed criminal acts performed by individuals (e.g., mens rea). These incidents can include a wide-range of activities that includes fraud, corruption, theft and illegal content. Criminal conduct generally involves one of the following kinds of mens rea: (1) intent, (2) knowledge, (3) recklessness and/or (4) negligence.
MT-15	Conflict of Interest (COI)	Conflict of Interest (COI) is a broad category but pertains to an ethical incompatibility. COI exist when (1) the concerns or goals of different parties are incompatible or (2) a person in a decision-making position is able to derive personal benefit from actions taken or decisions made in their official capacity.
MT-16	Macroeconomics	Macroeconomic factors that can negatively affect the global supply chain. Macroeconomic factors directly impact unemployment rates, interest rates, exchange rates and commodity prices. Due to how fiscal and monetary policies can negatively affect the global supply chain, this can disrupt or degrade an organization's business operations.
MT-17	Foreign Ownership, Control, or Influence (FOCI)	Foreign Ownership, Control, or Influence (FOCI) is a Supply Chain Risk Management (SCRM) threat category that pertains to the ownership of, control of, or influence over an organization. Primarily, the concern is if a foreign interest (e.g., foreign government or parties owned or controlled by a foreign government) has the direct or indirect ability to influence decisions that affect the management or operations of the organization.
MT-18	Geopolitical	Geopolitical is a Supply Chain Risk Management (SCRM) threat category that pertains to a specific geographic location, or region of relevance, that affects the supply chain. Primarily, the concern is if a foreign state can affect the supply chain through political intervention within the host nation.
MT-19	Sanctions	Sanctions is a Supply Chain Risk Management (SCRM) threat category that pertains to past or present fraudulent activity or corruption. Primarily, the concern is if the third-party is subject to suspension, exclusion or other sanctions that can affect the supply chain.
MT-20	Counterfeit / Non-Conforming Products	Counterfeit / Non-Conforming Products is a Supply Chain Risk Management (SCRM) threat category that pertains to the integrity of components within the supply chain. Counterfeits are products introduced to the supply chain that falsely claim to be produced by the legitimate Original Equipment Manufacturer (OEM), whereas non-conforming are OEM products / materials that fail to meet the customer specifications. Both can have a detrimental effect on the supply chain.
MT-21	Operational Environment	Operational Environment is a Supply Chain Risk Management (SCRM) threat category that pertains to the user environment (e.g., place of performance). Primarily, the concern is if the operational environment is hazardous that could expose the organization operationally or financially.
MT-22	Supply Chain Interdependencies	Supply Chain Interdependencies is a Supply Chain Risk Management (SCRM) threat category pertaining to interdependencies related to data, systems and mission functions.
MT-23	Third-Party Quality Deficiencies	Third-Party Quality Deficiencies is a Supply Chain Risk Management (SCRM) threat category that provide insights into the ability of the third-party to produce and deliver products and/or services as expected. This includes an understanding of the quality assurance practices associated with preventing mistakes or defects in manufactured/ developed products and avoiding problems when delivering solutions or services to customers.

Section 14. Assessment Objectives (AOs)

The SCF contains an Assessment Objectives (AOs) tab to support the SCF Conformity Assessment Program (SCF CAP), since assessors must evaluate controls by utilizing AOs, when AOs are available.

An AO is an objective statement that establishes the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.



SCF #	SCF AO #	SCF Assessment Objective (AO) In addition to relevant policies, standards and procedures, the assessor shall examine, interview, and/or test to determine if appropriately scoped evidence exists to support the claim that:	SCF Assessment Objective (AO) Origin(s)	SCF Baseline AOs	DHS ZTCF AOs	NIST 800-53 R5 AOs	NIST 800-171 R2 AOs	NIST 800-171 R3 AOs	NIST 800-172 AOs
AAT-01	AAT-01_A01	Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific policies, standards and procedures are developed and documented.	SCF Created	x					
AAT-01	AAT-01_A02	Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific policies, standards and procedures are implemented effectively.	SCF Created	x					
AAT-01.1	AAT-01.1_A01	the organization analyzes its business practices to determine applicable statutory, regulatory and/or contractual obligations for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	SCF Created	x					
AAT-01.2	AAT-01.2_A01	secure engineering principles are defined.	53A_R5_SA-08_ODP[01]	x		x			
AAT-01.2	AAT-01.2_A02	privacy engineering principles are defined.	53A_R5_SA-08_ODP[02]	x		x			
AAT-01.3	AAT-01.3_A01	the organization analyzes its business practices for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	SCF Created	x					
AAT-01.3	AAT-01.3_A02	the organization continuously improves its business practices to sustain the value of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	SCF Created	x					
AAT-02	AAT-02_A01	an inventory of systems and system components that is at the level of granularity deemed necessary for tracking and reporting is documented.	53A_R5_CM-08a.04	x		x			
AAT-02.1	AAT-02.1_A01	a risk catalog of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific risks is documented.	SCF Created	x					
AAT-02.1	AAT-02.1_A02	a compliance catalog of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific laws, regulations and contractual obligations are documented.	SCF Created	x					
AAT-02.1	AAT-02.1_A03	the organization maps its risk catalog to its compliance catalog for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	SCF Created	x					
AAT-02.2	AAT-02.2_A01	roles and responsibilities exist to compel data and/or process owners to select required cybersecurity / data privacy controls for Artificial Intelligence (AI) and Autonomous Technologies (AAT) under their control.	SCF Created	x					
AAT-02.2	AAT-02.2_A02	Individual Contributor (IC) performance reviews cover how data and/or process owners operationalized cybersecurity / data privacy practices for Artificial Intelligence (AI) and Autonomous Technologies (AAT) under their control.	SCF Created	x					
AAT-03	AAT-03_A01	the context for the intended purpose(s) for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.	SCF Created	x					
AAT-03	AAT-03_A02	the context for the potentially beneficial use(s) for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.	SCF Created	x					
AAT-03	AAT-03_A03	the context for the legal and regulatory compliance for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.	SCF Created	x					
AAT-03	AAT-03_A04	the context for the norms and expectations for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.	SCF Created	x					
AAT-03	AAT-03_A05	the context for the proposed deployment setting(s) for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.	SCF Created	x					
AAT-03.1	AAT-03.1_A01	the mission for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.	SCF Created	x					
AAT-03.1	AAT-03.1_A02	the relevant goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are clearly documented.	SCF Created	x					
AAT-04	AAT-04_A01	capabilities for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are benchmarked.	SCF Created	x					

AO Origins

Each AO is tagged to identify its origin. The AOs may include one, or more, origins due to overlap:

- SCF created;
- NIST SP 800-53A R5;
- NIST SP 800-171A;
- NIST SP 800-171A R3; and
- NIST SP 800-172A.

Objective Assessment Criteria

AOs provide objective criteria that each must be satisfied to legitimately determine whether the control is implemented and operating as intended. A control cannot be designated as Satisfied unless all of the AOs are either:

- Satisfied;
- Not Applicable (N/A); or
- Compensating Control.

In the context of control designations, a designation of:

- Satisfactory is positive, where the criteria are met;
- Deficient is negative, where the criteria are not met;
- Compensating Control is neutral, where another control, or controls, is/are designated as sufficiently reducing the risk(s) associated with the control; and
- N/A is neutral, where the control, or AO, does not apply.

This guide is for educational purposes only. You are encouraged to work with a competent professional to validate any compliance-related assumptions.

SECTION 15. EVIDENCE REQUEST LIST (ERL)

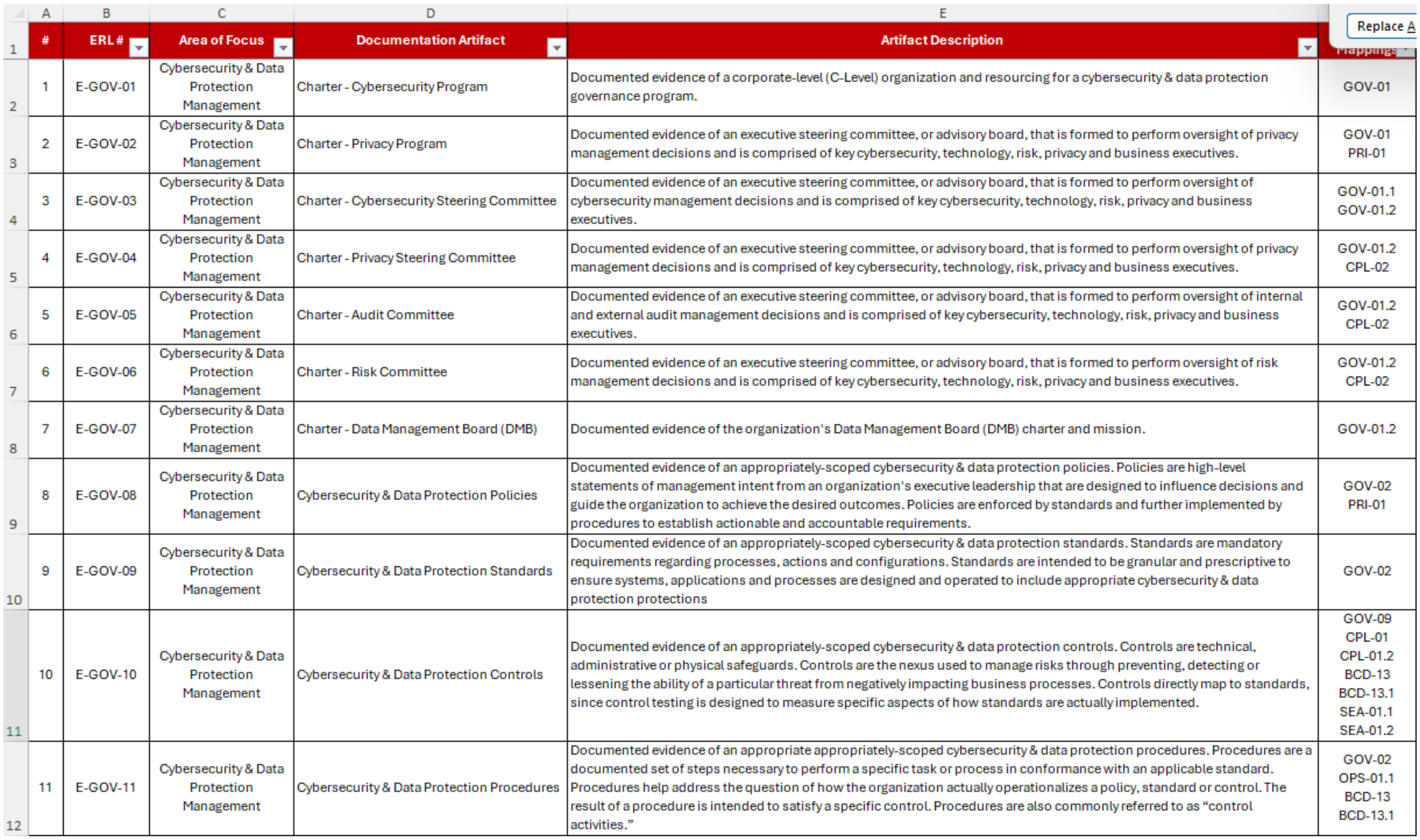
The SCF contains an Evidence Request List (ERL) tab to support the SCF Conformity Assessment Program (SCF CAP). The ERL:

- Represents the minimum level of reasonable evidence requests to perform a controls assessment;
- Establishes a finite list of supporting evidence used in an assessment; and
- Standardizes evidence expectations to allow Organizations Seeking Assessment (OSA) to have sufficient time to accumulate reasonable evidence to determine the adequacy of control design and operation.

REASONABLE ASSESSMENT ARTIFACTS

Assessors and Third-Party Assessment Organizations (3PAOs) operate from a position of trust and authority. Therefore, minimizing "scope creep" that can increase the duration, cost and personnel commitments associated with an assessment is essential. As part of due diligence activities, assessors and 3PAOs are expected to:

- Define an authoritative ERL; and
- Before the start of the assessment, provide any artifact requests to the OSA.



	A	B	C	D	E	
1	#	ERL #	Area of Focus	Documentation Artifact	Artifact Description	Mappings
2	1	E-GOV-01	Cybersecurity & Data Protection Management	Charter - Cybersecurity Program	Documented evidence of a corporate-level (C-Level) organization and resourcing for a cybersecurity & data protection governance program.	GOV-01
3	2	E-GOV-02	Cybersecurity & Data Protection Management	Charter - Privacy Program	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of privacy management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01 PRI-01
4	3	E-GOV-03	Cybersecurity & Data Protection Management	Charter - Cybersecurity Steering Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of cybersecurity management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.1 GOV-01.2
5	4	E-GOV-04	Cybersecurity & Data Protection Management	Charter - Privacy Steering Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of privacy management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
6	5	E-GOV-05	Cybersecurity & Data Protection Management	Charter - Audit Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of internal and external audit management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
7	6	E-GOV-06	Cybersecurity & Data Protection Management	Charter - Risk Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of risk management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
8	7	E-GOV-07	Cybersecurity & Data Protection Management	Charter - Data Management Board (DMB)	Documented evidence of the organization's Data Management Board (DMB) charter and mission.	GOV-01.2
9	8	E-GOV-08	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Policies	Documented evidence of an appropriately-scoped cybersecurity & data protection policies. Policies are high-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes. Policies are enforced by standards and further implemented by procedures to establish actionable and accountable requirements.	GOV-02 PRI-01
10	9	E-GOV-09	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Standards	Documented evidence of an appropriately-scoped cybersecurity & data protection standards. Standards are mandatory requirements regarding processes, actions and configurations. Standards are intended to be granular and prescriptive to ensure systems, applications and processes are designed and operated to include appropriate cybersecurity & data protection protections	GOV-02
11	10	E-GOV-10	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Controls	Documented evidence of an appropriately-scoped cybersecurity & data protection controls. Controls are technical, administrative or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes. Controls directly map to standards, since control testing is designed to measure specific aspects of how standards are actually implemented.	GOV-09 CPL-01 CPL-01.2 BCD-13 BCD-13.1 SEA-01.1 SEA-01.2
12	11	E-GOV-11	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Procedures	Documented evidence of an appropriate appropriately-scoped cybersecurity & data protection procedures. Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard. Procedures help address the question of how the organization actually operationalizes a policy, standard or control. The result of a procedure is intended to satisfy a specific control. Procedures are also commonly referred to as "control activities."	GOV-02 OPS-01.1 BCD-13 BCD-13.1

SECTION 16. POSSIBLE SOLUTIONS & CONSIDERATIONS

The SCF leveraged the firm size model from the Bureau of Labor Statistics (BLS) to organize possible solutions and considerations for applicable SCF controls.[48] The SCF consolidated the nine (9) BLS firm sizes into five (5):

1. Micro-Small Business;
2. Small Business;
3. Medium Business;
4. Large Business; and
5. Enterprise.

SOLUTIONS FOR MICRO-SMALL BUSINESS

The micro-small business category is applicable to organization that:

- Have less than ten (10) employees; or
- Are in BLS Firm Size Classes 1-2.

SOLUTIONS FOR SMALL BUSINESS

The small business category is applicable to organization that:

- Have between ten (10) and forty-nine (49) employees; or
- Are in BLS Firm Size Classes 3-4.

SOLUTIONS FOR MEDIUM BUSINESS

The medium business category is applicable to organization that:

- Have between fifty (50) and two hundred forty-nine (249) employees; or
- Are in BLS Firm Size Classes 5-6.

SOLUTIONS FOR LARGE BUSINESS

The large business category is applicable to organization that:

- Have between two hundred fifty (250) and nine hundred ninety-nine (999) employees; or
- Are in BLS Firm Size Classes 7-9.

SOLUTIONS FOR ENTERPRISES

The enterprise category is applicable to organization that:

- Have one thousand or more (1,000+) employees; or
- Are in BLS Firm Size Classes 9.

EXPERT INSIGHT (POSSIBLE SOLUTIONS): For most SCF controls, the solutions would be to have administrative controls such as documented policies, standards and procedures. It would be highly inefficient and add no value to have that common assumption written for every control, so the focus was on unique administrative, physical and/or technical solutions that may be applicable for a specific control, beyond the assumed policies, standards and procedures.

[48] *BLS Firm Size Classes - https://www.bls.gov/bdm/bdmfirmsize.htm*

SECTION 17. PRE-DEFINED CONTROL SETS

The SCF has several “pre-defined control sets” that contain a subset of the SCF catalog where those controls are specific to a unique business need.

Those pre-defined control sets are:

- SCF CORE Fundamentals;
- SCF CORE Mergers, Acquisitions & Divestitures (MA&D);
- SCF CORE ESP Level 1 – Foundational;
- SCF CORE ESP Level 2 – Critical Infrastructure;
- SCF CORE ESP Level 3 – Advanced Threats;
- SCF CORE AI-Enabled Operations; and
- SCF CORE AI Model Deployment.

These are “good idea fairy” starting points for those who may want a push in the right direction for possible controls to address these pre-defined topics.

SECTION 18. FREQUENTLY ASKED QUESTIONS (FAQ)

The SCF is more than just an assortment of cybersecurity and data privacy controls. The SCF is focused on (1) designing, (2) implementing and (3) maintaining SECURE & COMPLIANT solutions to address all applicable statutory, regulatory and contractual requirements that an organization faces.

The SCF Council's is confident is that if an organization properly scopes its cybersecurity and data protection requirements with security in mind, compliance will often be a natural byproduct of those actions. To properly use the SCF to become secure and compliant, it requires an organization's users to understand what the SCF is and how to use it. Therefore, these FAQs are published for that purpose.

GENERAL FAQ

This section addresses general FAQ associated with the SCF.

GEN-FAQ-001: HOW DO I START USING THE SCF?

Before you dive into the SCF, it is imperative that you understand the fundamentals of what the SCF is and what it is not. Without that knowledge, you will likely use the SCF incorrectly (e.g., trying to use a screwdriver as a prybar). You can gain this understanding through reading the SCF Overview & Instructions document. If you do not want to take the time to educate yourself on the basics, you are advised to avoid using the SCF and find a different solution for your needs or outsource the work to a competent third-party.

You access the SCF in one (1) of two (2) ways:

1. Download the Excel version from the SCF website; or
2. Use a GRC tool, such as SCF Connect or others listed on the SCF Marketplace.

If you get stuck, there are a few resources available:

1. Re-read the SCF Overview & Instructions to see if you missed something;
2. Sign up for the SCF Discord server to ask questions;
3. Hire a SCF Trainer from the SCF Marketplace to provide individual or group training; and/or
4. Hire a SCF Practitioner or SCF Architect from the SCF Marketplace to get 1-1 consulting expertise.

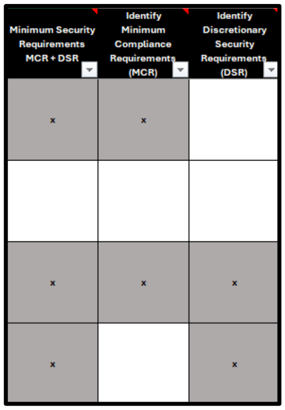
While the SCF Council gives away the SCF for free, if you want a consultant to take you through setting up or operationalizing your control set, you will have to pay for that service. The SCF Marketplace has a non-exclusive listing of cybersecurity and data privacy professionals who have the skills and experience to assist you.

GEN-FAQ-002: HOW DO I SELECT CONTROLS SPECIFIC TO MY NEEDS?

The SCF is fundamentally an Excel spreadsheet. Therefore, you can use your Excel skills to manually filter the requirements. If you are comfortable with Excel, it might take you 5-10 minutes to do this filtering, based on how many requirements you need to map to. Within the SCF, there is a column labelled "Minimum Security Requirements (MSR) MCR + MSR" that will assist you in this process.

Follow these steps to tailor the SCF:

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).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).
2. A selection of either MCR or DSR will automatically select the MSR + DSR column:
    a. In the MCR column, simply put an "x" to mark that control as being "must have" controls.
    b. In the DSR column, simply put an "x" to mark that control as being "nice to have" controls.
3. Unfilter the column you just performed this task on and do it to the next law, regulation or framework that you need to map.
4. Repeat steps 2 and step 3 until all your applicable laws, regulations and frameworks are mapped to.



Minimum Security Requirements MCR + DSR	Identify Minimum Compliance Requirements (MCR)	Identify Discretionary Security Requirements (DSR)
x	x	
x	x	x
x		x

The MSR + DSR column will now have an “x” that marks each SCF control that is applicable for your needs, based on what was selected for MCR and DSR controls. This will leave you with a SCF control set that is tailored for your specific needs.

GEN-FAQ-003: How Often Is The SCF Updated?

The general cadence for updates is one (1) update per quarter (e.g., four (4) updates per year). There may be situations where out-of-cycle updates are released, but the goal is to publish updates on a quarterly basis.

GEN-FAQ-004: Why Is The SCF Free To Use?

The SCF is free to help fix the broken nature of cybersecurity and data privacy practices that many organizations face. The reality is that we cannot rely on politicians to fix anything, so it is up to us to provide solutions.

The quality of the SCF could easily justify a costly subscription service, but we know that would exclude most organizations and defeat our broader goal of improving cybersecurity and data privacy practices on a macro scale. While our contributors are volunteers, we rely on our generous sponsors to maintain the SCF.

GEN-FAQ-005: What Does "Mechanisms Exist" Mean?

The controls that make up the SCF were written to (1) be flexible and (2) meet the needs of organizations, regardless of size or industry. That approach to control structure can make wording a challenge. One solution that SCF architects came to agreement on is in the approach to normalizing control wording. For example:

- "Mechanisms exist to..."
- "Automated mechanisms exist to..."
- "Physical security mechanisms exist to..."

The use of the term “mechanism” is the best option, since a mechanism can mean (1) a manual process, (2) a technology solution, (3) outsourced contract or (4) a combination of those that come together to address the needs of the control. Some smaller companies may lack technology solutions for many controls, so manual processes will likely prevail. However, getting into Fortune 500 environments, technology solutions will most often exist to address the controls.

GEN-FAQ-006: Are There Restrictions On The Use of the SCF?

Yes. The Secure Controls Framework is copyrighted material, but it leverages the Creative Commons Attribution-NoDerivatives 4.0 International Public License to help maintain the integrity of the SCF. Under the SCF Terms & Conditions:

- Attribution - You must give appropriate credit, provide a link to the license and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. Providing attribution is as simple as stating SCF controls are used in the solution, such as a GRC platform that includes SCF content is required to provide attribution that SCF controls are used.
- NoDerivatives - If you remix, transform, or build upon the material, you may not distribute the modified material. For example, you are prohibited from leveraging SCF material to create a derivative solution (e.g., SCF 2.0). This prohibition on creating derivative works includes utilizing Artificial Intelligence (AI) (or similar technologies) to leverage SCF content to generate policies, standards, procedures, metrics, risks, threats or other derivative content.

GEN-FAQ-007: How Does The Control Weighting Work In The SCF?

The SCF assigns a value on a scale from 1-10, with 1 being the least important and 10 being the most important. These values are subjective, based on SCF contributor discussion, since control weighting is important to help prioritize controls and assist with the understanding what really matters from a risk management perspective. For an insight into the thought process, a control weighting of 10 was framed as *“Would you do business with an organization that did not have this control in place?”* where certain controls were identified as an absolute minimum from a risk threshold perspective from a “reasonable person” perspective.

- Those controls designated as a score of 10 should be considered a MATERIAL / KEY CONTROL (e.g., lack of or a deficiency should be considered a material weakness).
- On the opposite side of the spectrum, a score of 1 was deemed “nice to have” but did not materially affect risk.

GEN-FAQ-008: Why Does The SCF Say It Is The Common Controls Framework?

The use of Common Controls Framework™ is trademarked by the SCF. The SCF has exclusive rights to say the SCF is the Common Controls Framework™. Additionally, the following domains point to the SCF's website:

- common-controls-framework.com; and
- commoncontrolsframework.com

GEN-FAQ-009: What Is The Cybersecurity & Data Protection Assessment Standards (CDPAS)?

The Secure Control Framework Council (SCF Council) established a cohesive, consistent set of standards for performing cybersecurity and data protection-related Third-Party Assessment, Attestation and Certification Services (3PAAC Services). By following the Cybersecurity & Data Protection Assessment Standards (CDPAS) approach, cybersecurity and data protection practitioners can improve the currently disjointed approach used to perform assessments of cybersecurity and/or data protection controls.

The CDPAS is a "standard" that normalizes third-party assessment practices. Per NIST, a standard is "a document, established by consensus and approved by a recognized body, which provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context."

Conformity Assessment Program (CAP) FAQ

This section addresses general FAQ associated with the SCF CAP.

CAP-FAQ-001: What Is The SCF CAP?

The SCF Conformity Assessment Program (SCF CAP) is an organization-level conformity assessment. The SCF CAP is designed to utilize tailored cybersecurity and data privacy controls that specifically address the applicable statutory, regulatory and contractual obligations an Organization Seeking Assessment (OSA) is required to comply with. By using the metaframework nature of the SCF, an OSA is able to perform conformity assessment that spans multiple cybersecurity and data privacy-specific laws, regulations and frameworks.

The SCF CAP is focused on using the SCF as the control set to provide a company-level certification. While the SCF-CAP shares some similarities with other existing, single-focused certifications (e.g., ISO 27001, CMMC, FedRAMP, etc.), the SCF CAP is unique in its metaframework approach to covering cybersecurity and data protection requirements that span multiple laws, regulations and frameworks

CAP-FAQ-002: What Is A Conformity Assessment?

NIST Special Publication 200-01, *ABC's of Conformity Assessment*, is where you should start to understand what a conformity assessment is and why it is important. That document is designed to provide the reader with an introduction to conformity assessment and information on how the various conformity assessment activities are interlinked.