SECURE CONTROLS FRAMEWORK

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

version 2023.3

con·trol
/kən trol/

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

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

Table of Contents

EXECUTIVE SUMMARY

Thank you for you interest in the **Secure Controls Framework's™ (SCF) Security & Privacy Capability Maturity Model (SP-CMM)**! The SP-CMM is built directly into the SCF and is free to downloaded from https://www.securecontrolsframework.com.

This was a massive undertaking by SCF contributors to define maturity levels for the SCF's control catalog. The result of that work is each of the SCF's controls has corresponding L0-5 criteria defined. *Note – the 2023.2 version of the SCF contains refreshed SP-CMM content.*

This document is designed for cybersecurity & privacy practitioners to gain an understanding of what the SP-CMM is and how it can be used in their organization.

Just like the SCF itself, the SP-CMM is free for organizations to use through the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) license.

OBJECTIVES OF THE SP-CMM

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

1. Provide CISO/CPOs/CIOs with objective criteria that can be used to establish expectations for a cybersecurity & privacy program;
2. Provide objective criteria for project teams so that secure practices are appropriately planned and budgeted for;
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 privacy practices as part of Mergers & Acquisitions (M&A).

There are likely many other use cases that the SP-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 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.

NOT JUST ANOTHER CMM

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 SP-CMM draws upon the high-level structure of the **Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM)**, since we felt it was the best model to demonstrate varying levels of maturity for people, processes and technology at a control level. If you are unfamiliar with the SSE-CMM, it is well-worth your time to read through the *SSE-CMM Model Description Document* that is hosted by the US Defense Technical Information Center (DTIC).[1]

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).*[2]

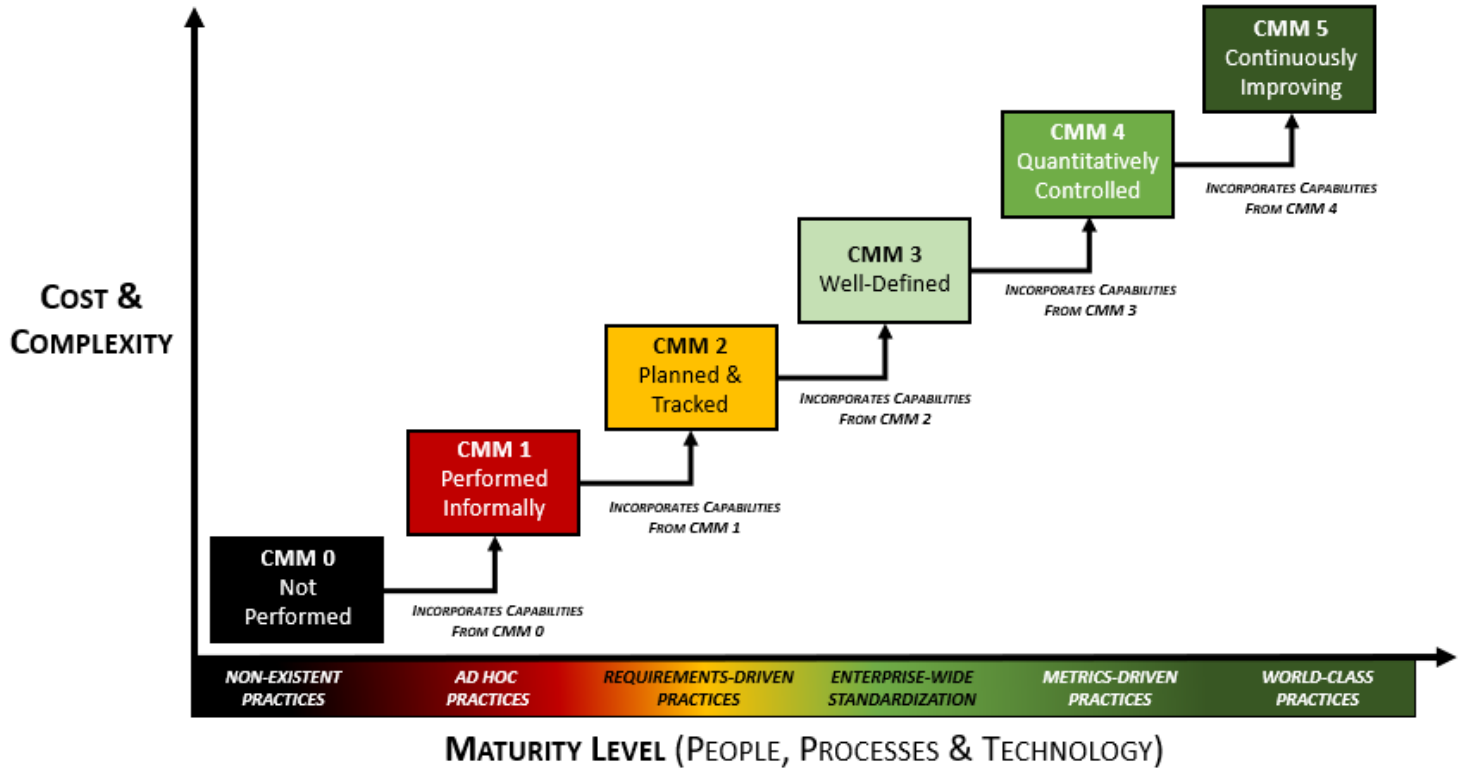
NESTED APPROACH TO MATURITY

By using the term "nested" regarding maturity, we refer to how the SP-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 SP-CMM is structured.

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

Security & Privacy Capability Maturity Model (SP-CMM) Overview

The SP-CMM draws upon the high-level structure of the **Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM)**, since we felt it was the best model to demonstrate varying levels of maturity for people, processes and technology at a control level. If you are unfamiliar with the SSE-CMM, it is well-worth your time to read through the *SSE-CMM Model Description Document* that is hosted by the US Defense Technical Information Center (DTIC).[3]



Maintaining The Integrity of Maturity-Based Criteria

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."*[4]

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 SP-CMM.

Divining A Maturity Level Decision From Control-Level Maturity Criteria

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 SP-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.

---

[3] *Defense Technical Information Center (DTIC) - https://apps.dtic.mil/dtic/tr/fulltext/u2/a393329.pdf*

[4] *US Department of Justice - https://www.justice.gov/archives/jm/criminal-resource-manual-1007-fraud*

MATURITY (GOVERNANCE) ≠ ASSURANCE (SECURITY)

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."*[5] 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:

- **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 SP-CMM LEVELS

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

SP-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[6] and due diligence[7] 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.*

SP-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

---

[5] *US Department of Justice - https://www.justice.gov/archives/jm/criminal-resource-manual-1007-fraud*

[6] *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.*

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

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.*

SP-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 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.*

SP-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 (note - 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 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.*

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

SP-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:

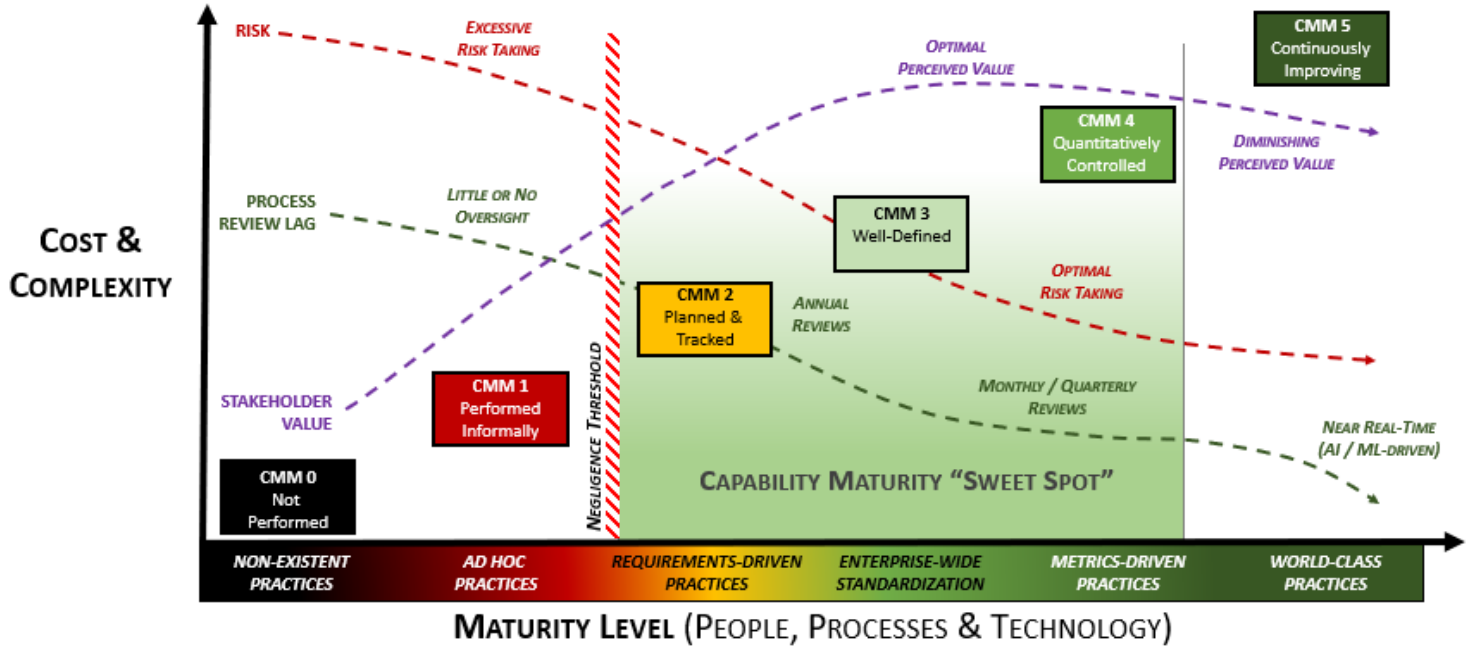
- *For small and medium-sized organizations, it is unrealistic to attain this level of maturity.*
- *For large organizations:*
  - *IT staff have clear requirements to implement standardized cybersecurity & privacy principles across the enterprise.*
  - *In addition to the existence of a dedicated cybersecurity 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 privacy program (e.g., quarterly business reviews to the CIO/CEO/board of directors). This situational awareness is made possible through detailed metrics.*
  - *The organization has a very aggressive business model that requires not only IT, but its cybersecurity and privacy practices, to be innovative to the point of leading the industry in how its products and services are designed, built or delivered.*
  - *The organization invests heavily into developing AI/ML technologies to 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 privacy teams dictating targets. Identifying maturity targets is meant to be a team effort between both technologists and business stakeholders.

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

Note - During the development of the SP-CMM, a contributor identified an interesting insight that L0-L3 are "internal" maturity levels for cybersecurity and 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 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).

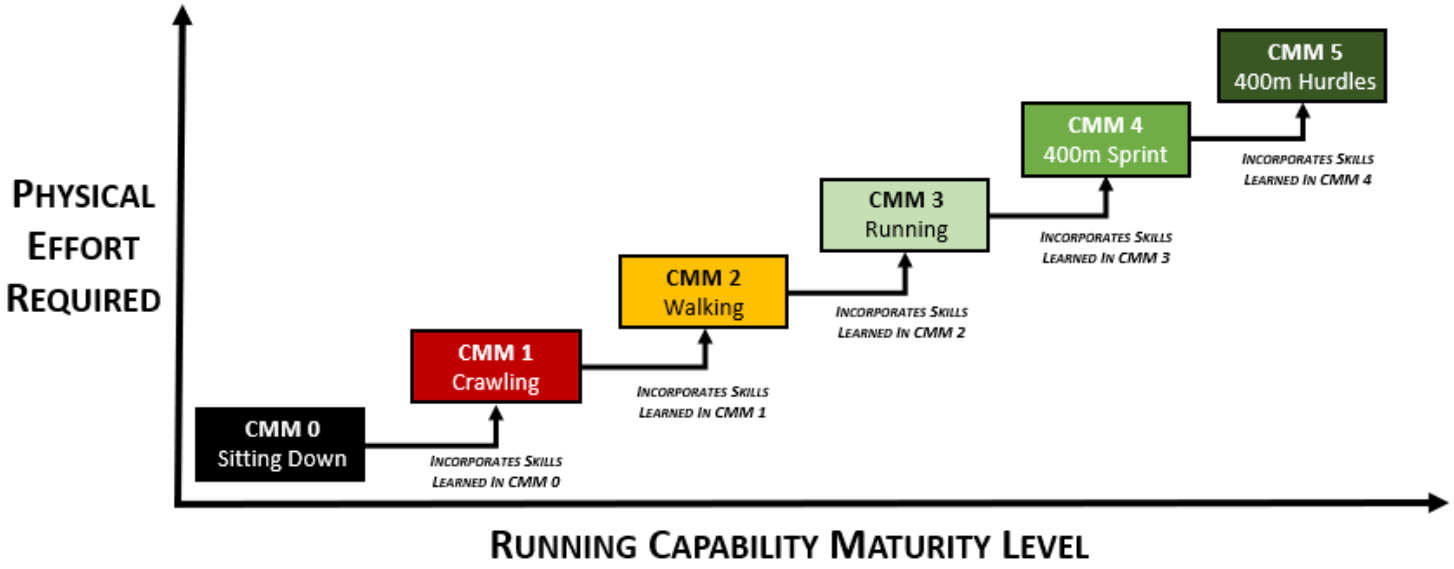
Stakeholder Value Considerations

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.

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.



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

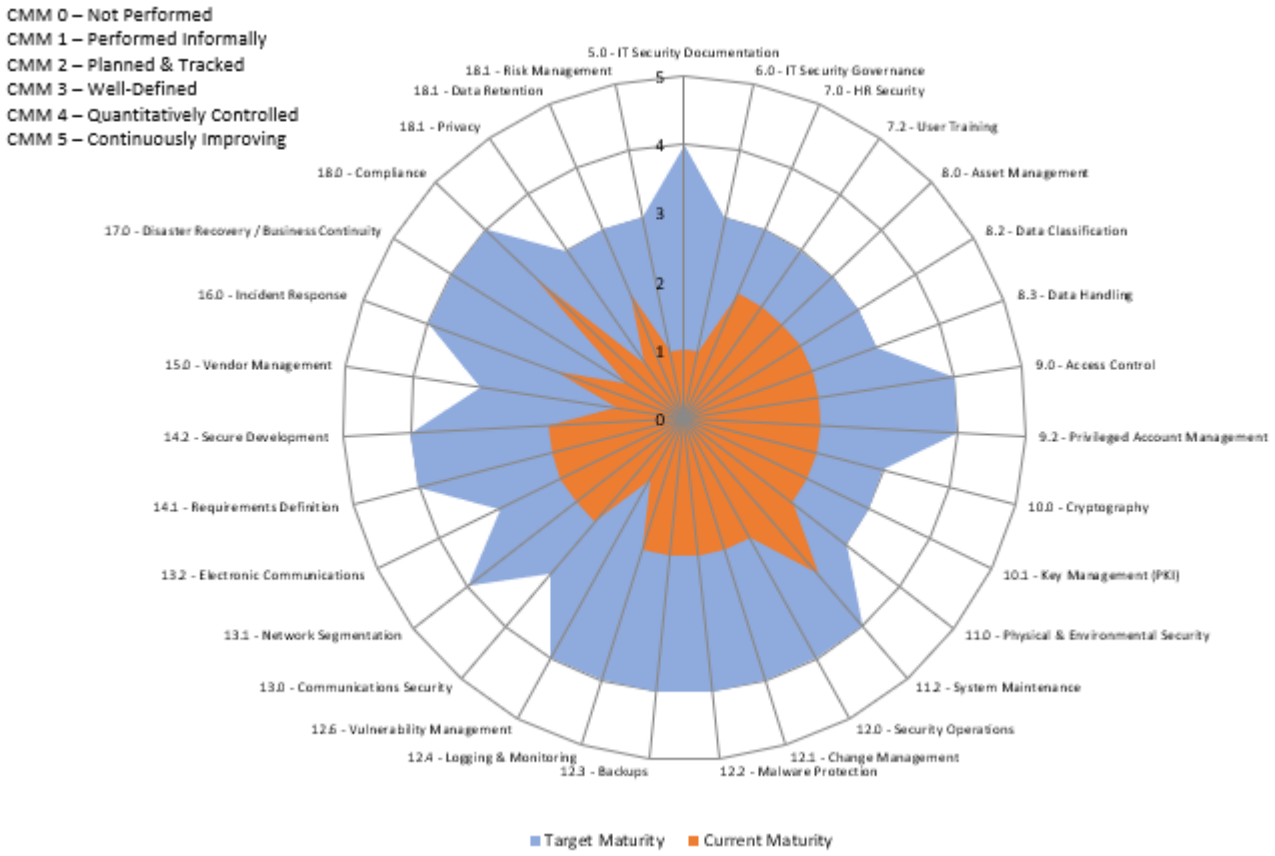
- **L0 – Sitting Down**
  - Sitting down would be non-existent effort. No evidence of exercise exists.
  - Sitting down would be considered deficient in terms of meeting this control.
- **L1 – Crawling**
  - Crawling is at best considered ad-hoc exercise and likely doesn't meet the intent of the control.
  - 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.

EXPECTED SP-CMM USE CASES

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

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

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



IDENTIFYING THE PROBLEM

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

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

CONSIDERATIONS

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

When identifying a target level of maturity, it is crucial to account for your organization's culture. The reason for this is the implementation of perceived "draconian" levels of security can cause a revolt in organizations not accustomed to heavy restrictions. One good rule of thumb when deciding between 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

Defining a target maturity state is Step 4 in the Integrated Controls Management (ICM) model is a free resource from the SCF. That guide can be useful, since it helps establish two key pre-requisites to identifying CMM targets:

1. Prioritization of efforts (including resourcing); and
2. Identification of applicable statutory, regulatory and contractual obligations.

The most efficient manner we can recommend would be to first look at the thirty-two domains that make up the SCF and assign a high-level CMM level target for each domain. These domains are well-summarized in the SCF's free Security & Privacy by Design Principles (SIP) document and can be used by a CISO/CIO/CPO to quickly align a maturity target to each domain, in accordance with previously-established prioritization and business needs.

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 privacy by default and by design. In order to determine what is appropriate and to evaluate it prior to "go live" it necessitates expectations for control maturity to be defined.

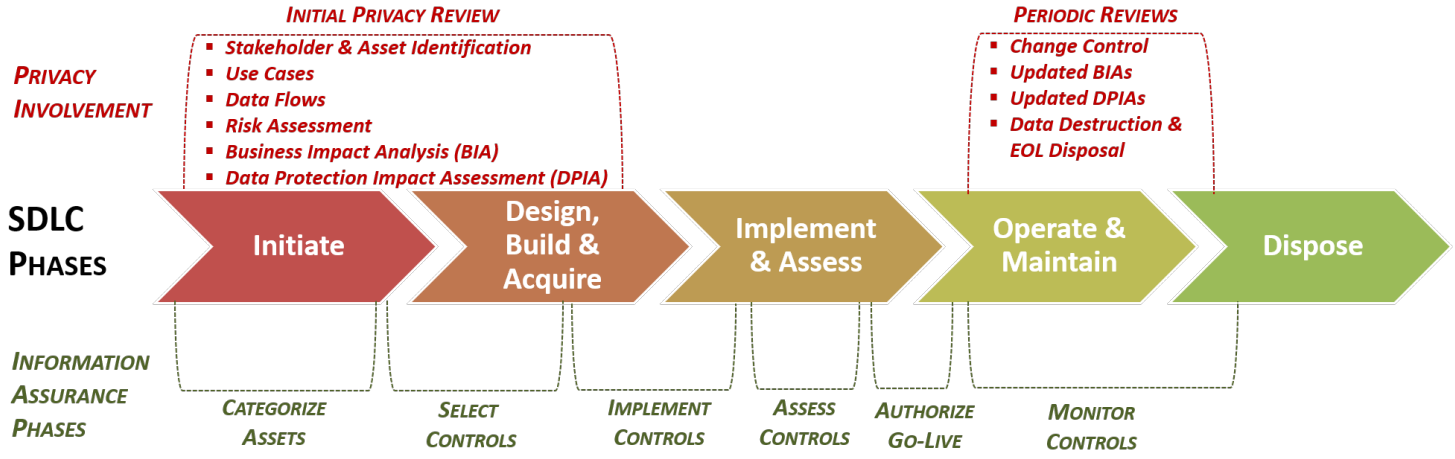
Identifying The Problem

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

Considerations

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



Projects do not have unlimited budgets, nor do they tend to have overly flexible timelines that allow for new security & privacy tools to be installed and trained upon. From a project perspective, this is often going to limit target CMM levels to L2-3 for planning purposes.

Identifying A Solution

While there are over 1,000 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). In the end, the result is a tailored set of controls that meet 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 Third-Party Service Providers (TSPs), including vendors and partners, to be contractually bound to implement and manage a baseline set of cybersecurity and privacy controls. This necessitates oversight of TSPs to ensure controls are properly implemented and managed.

Identifying The Problem

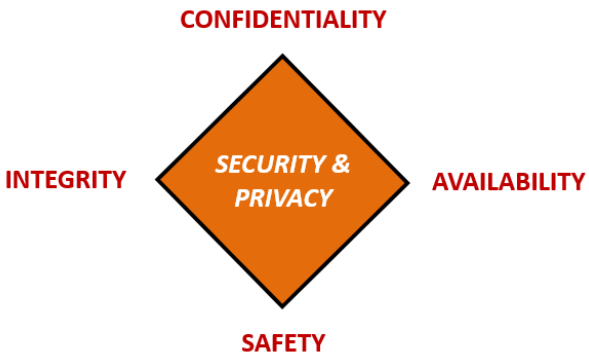
In managing a cybersecurity and privacy program, it is important to address controls in a holistic manner, which includes governing the supply chain. TSPs are commonly considered the "soft underbelly" for an organization's security program, since TSP oversight has traditionally been weak or non-existent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

One of the issues with managing TSPs is most questionnaires ask for simple yes, no or not applicable answers. This approach lacks details that provide critical insights into the actual security posture of the TSP. The SP-CMM can be used to obtain more nuanced answers from TSPs by having those TSPs select from L0-5 to answer if the control is implemented and how mature the process is.

Considerations

Referencing back to the SP-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 TSPs need to be able to demonstrate to properly protect your systems, applications, services and data, regardless of where it is stored, transmitted or processed. From a TSP management perspective, this is often going to limit target CMM levels to L2-3 for most organizations.

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



Identifying A Solution

While there are over 1,000 controls in the SCF's controls catalog, it is necessary to pare down that catalog to only what is applicable to that specific TSP'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). In the end, the result is a tailored set of controls that address the TSP'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 TSP. Ideally, the TSP 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 TSP-specific controls is appropriate.

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

It is commonplace to conduct a cybersecurity and 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 privacy practices. That is why the SCF-B is a bespoke set of cybersecurity and privacy controls that was purposed built for M&A to provide as complete a picture as possible about the divesting entity's cybersecurity and 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 SP-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 SP-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-premise, cloud and hybrid architectures)
- 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
- EU GDPR