SECURE CONTROLS FRAMEWORK

SCF Overview & Practitioner Guidebook

version 2026.3

This document is designed for security, compliance and resilience 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. Users 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

Executive Summary 5

Section 1. Terminology & Acronyms 6

Terminology Standardization 6

Acronyms 11

Section 2. Introduction To The Secure Controls Framework® 16

Why Should An Organization Use The SCF? 16

Integrated Controls Management (ICM) Mindset 17

What The SCF Is 17

What The SCF Is Not 17

Addressing The Who? What? Where? When? Why? and How? 18

Section 3. Understanding Fundamental Governance, Risk & Compliance (GRC) Functions 19

GRC Is A Plan, Do, Check & Act (PDCA) Adventure – That Is A Concept that Should Be Embraced, Not Fought Against 19

People, Processes, Technology, Data, Facilities and Artificial Intelligence (PPTDF-AI) 20

Chicken vs Egg Debate: The Logical Order of GRC Functions 21

Compliance 21

Governance 22

Risk Management 23

Section 4. Control Weighting, Tailoring & Compensating Controls 24

SCF Control Weighting Explanation 24

Tailoring Is Required - Not All Controls Are Applicable 24

Statutory Requirements 25

Regulatory Requirements 25

Contractual Requirements 25

Tailoring SCF Controls - Defining "Must Have" vs "Nice To Have" Controls 26

Compensating Controls 27

Compensating Control Considerations 27

What Compensating Controls Are 28

What Compensating Controls Are Not 28

Materiality Considerations For Compensating Controls 28

Section 5. Designing & Building An Audit-Ready Cybersecurity Program 30

Holistic Approach To Address Control Applicability 30

NIST IR 8477 - Set Theory Relationship Mapping (STRM) 30

STRM Relationship Types 31

STRM Relationship Type #1: SUBSET OF 31

STRM Relationship Type #2: INTERSECTS WITH 32

STRM Relationship Type #3: EQUAL 32

STRM Relationship Type #4: SUPERSET OF 32

STRM Relationship Type #5: NO RELATIONSHIP 32

Expert-Derived Content (EDC) vs Natural Language Processing (NLP) 32

Section 6. Secure, Compliant & Resilient Management System (SCRMS) 33

IT General Controls (ITGC) 34

Security vs Compliance 34

This concept of identifying a negligence threshold is addressed in the SCF's 34

MUST HAVE CONTROLS - Defining "Being Compliant" That Is Specific To Your Business Processes 35

NICE TO HAVE CONTROLS - Defining "Being Secure & Resilient" That Is Specific To Your Business Processes 35

Discretionary Security Considerations 35

Discretionary Resilience Considerations 35

Defining Negligence As It Pertains To Security, compliance and resilience 36

Determining A Breach Of Duty 36

Determining Whether There Was A Duty To Act 36

SCRMS Principles 37

SCRMS Principle 1: Establish Context 37

SCRMS Principle 2: Identify Applicable Controls 38

SCRMS Principle 3: Define Maturity Expectations 39

SCRMS Principle 4: Publish Governance Documentation 39

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SCRMS Principle 5: Assign Stakeholder Accountability 40
SCRMS Principle 6: Prioritize Capabilities According To Risk 40
SCRMS Principle 7: Maintain Situational Awareness 41
SCRMS Principle 8: Manage Risk 41
SCRMS Principle 9: Evolve Processes 42
Section 7. Secure, Compliant & Resilient Capability Maturity Model (SCR-CMM) 44
Well Established Maturity Model 44
Nested Approach To Maturity 44
Maturity (Governance) ≠ Assurance (Security) 45
Defining SCR-CMM Levels 45
SCR-CMM Level 0 (L0) - Not Performed 46
SCR-CMM Level 1 (L1) - Performed Informally 46
SCR-CMM Level 2 (L2) - Planned & Tracked 46
SCR-CMM Level 3 (L3) - Well Defined 47
SCR-CMM Level 4 (L4) - Quantitatively Controlled 48
SCR-CMM Level 5 (L5) - Continuously Improving 48
Defining A Capability Maturity "Sweet Spot" 49
Negligence Considerations 49
Risk Considerations 49
Process Review Lag Considerations 50
Stakeholder Value Considerations 50
Analog Example – Sit / Crawl / Walk / Run / Sprint / Hurdle 50
Maturity Model Use Cases 51
Use Case #1 – Objective Criteria To Build A Cybersecurity & Privacy Program 51
Use Case #2 – Assist Project Teams To Appropriately Plan & Budget Secure Practices 52
Use Case #3 – Provide Objective Criteria To Evaluate Third-Party Service Provider Security 53
Use Case #4 – Due Diligence In Mergers & Acquisitions (M&A) 54
Section 8. Secure, Compliant & Resilient Risk Management Model (SCR-RMM) 56
Risk Management Discussion Protections 57
Baselining Risk Management Terminology 59
Understanding The Differences: Threats vs Vulnerabilities vs Risks 60
Understanding The Differences Between: Risk Tolerance vs Risk Threshold vs Risk Appetite 61
Risk Management Options 65
Practical Risk Management Example 66
Summarizing The Integration Of Risk Management & Business Planning 66
Risk Management: Strategic Considerations 67
Risk Management: Operational Considerations 68
Risk Management: Tactical Considerations 68
Section 9. Risk & Threat Catalogs 70
SCF Risk Catalog 70
SCF Threat Catalog 75
Natural Threats 75
Manmade Threats 76
Section 10. Evidence Request List (ERL) 79
Reasonable Assessment Artifacts 79
Section 11. Assessment Objectives (AOs) 80
AO Origins 80
Objective Assessment Criteria 80
Section 12. Possible Solutions & Considerations 81
Solutions for Micro-Small Business 81
Solutions for Small Business 81
Solutions for Medium Business 81
Solutions for Large Business 81
Solutions for Enterprises 81
Section 13. Pre-Defined Control Sets 82
Section 14. Understanding What It Means To Adopt "Secure by Design" Principles 83
Secure Practices Are Common Expectations 83

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Compliance Should Be Viewed As A Natural Byproduct of Secure Practices 83
Secure, Compliant & Resilient (SCR) Principles 84
Steps To Operationalize The SCR Principles *84*
SCF Domains & SCR Principles *84*
Section 15. Understanding What It Means To Adopt "Privacy by Design" Principles 90
SCF Data Privacy Management Principles (DPMP) 90
Section 16. SCF Cybersecurity & Data Protection Assessment Standards (CDPAS) 92
CDPAS Purpose 92
CDPAS Intent 92
CDPAS Standards 92
Section 17. SCF Mergers, Acquisitions & Divestitures (MA&D) Security Standard (MADSS) 93
MADSS Purpose 93
MADSS Intent 93
MADSS Standards 93
Section 18. Secure Controls Framework Conformity Assessment Program (SCR CAP) 94
SCR CAP Body of Knowledge (SCR CAP BoK) 94
ABC's of Conformity Assessment 94
SCR CAP Ecosystem 95
The Cyber AB & Cyber EF *95*
SCR Assessor and Instructor Certification Organization (SAICO) *96*
The SCF Council *96*
Section 19. SCF Training & Individual Certifications 97
SCR Practitioner 97
SCR Architect 97
SCR Assessor 97
SCR Trainer 97
Section 20. Frequently Asked Questions (FAQ) 98
General FAQ 98
GEN-FAQ-001: How Do I Start Using The SCF? *98*
GEN-FAQ-002: How Do I Select Controls Specific To My Needs? *98*
GEN-FAQ-003: How Often Is The SCF Updated? *99*
GEN-FAQ-004: Why Is The SCF Free To Use? *99*
GEN-FAQ-005: What Does "Mechanisms Exist" Mean? *99*
GEN-FAQ-006: Are There Restrictions On The Use of the SCF? *99*
GEN-FAQ-007: How Does The Control Weighting Work In The SCF? *99*
GEN-FAQ-008: Why Does The SCF Say It Is The Common Controls Framework? *100*
GEN-FAQ-009: What Is The Cybersecurity & Data Protection Assessment Standards (CDPAS)? *100*
Conformity Assessment Program (CAP) FAQ 100
CAP-FAQ-001: What Is The SCR CAP? *100*
CAP-FAQ-002: What Is A Conformity Assessment? *100*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Executive Summary

With cybersecurity, we face a protracted war on an asymmetric battlefield. This problem is only further exacerbated with the weaponization of Artificial Intelligence (AI) technologies. The Secure Controls Framework (SCF) has three (3) key goals:

1. Minimize an organization's attack surface;
2. Provide the roadmap for an organization to be secure, compliant and resilient; and
3. Promote "defensible evidence" of reasonable practices.

Defensible evidence is the verifiable and objective proof that your organization's security, compliance and resilience activities:

- Actually occurred;
- Were effective; and
- Can withstand external scrutiny.

Defensible evidence can be viewed as on-demand assurance for stakeholders, where assurance is:

- Evidence-based confidence; and
- The demonstrable output of security, compliance and resilience activities.

Security + Compliance + Resilience needs to be a unified objective with a multi-discipline approach for security, compliance & resilience. This approach signals that an organization isn't just secure but:

- Meets its compliance requirements; and
- Can quickly bounce back from incidents.

The SCF is a comprehensive cybersecurity and data privacy metaframework designed to help organizations build secure, compliant and resilient capabilities. Instead of managing multiple, overlapping laws, regulations and frameworks independently, the SCF normalizes requirements into a Common Controls Framework (CCF) that supports multiple statutory, regulatory and contractual compliance requirements.

The SCF is free for businesses to use per the Creative Commons licensing model. The SCF can be downloaded as an Excel spreadsheet from the SCF website or GitHub. The current version of the SCF contains:

- 34 domains
- 1,500+ Controls
- Crosswalk mapping to over 200 laws, regulations and frameworks
- Control weighting
- Control questions
- Maturity Model Criteria
- Risk catalog
- Threat catalog
- Evidence Request List (ERL)
- Assessment Objectives (AOs)
- People, Process, Data, Technology & Facilities (PPTDF) Associations
- Data Privacy Management Principles

The SCF utilizes Set Theory Relationship Mapping (STRM) from NIST IR 8477 to create defensible mappings, so there is transparency with the SCF that other frameworks lack. You can see for yourself why one or more SCF controls map to a requirement from a specific law, regulation or framework. By normalizing controls across laws, regulations, and industry standards, the SCF enables organizations to reduce compliance complexity while improving security program effectiveness. The SCF helps organizations implement practical safeguards, generate defensible evidence of control effectiveness and demonstrate accountability to regulators, customers and other stakeholders.

With the SCF, cybersecurity becomes more than compliance, where it becomes a sustainable system for managing risk, protecting information and ensuring operational resilience in an increasingly complex threat and regulatory environment.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

This guide is for educational purposes only. Users 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 security, compliance and resilience 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 security, compliance and resilience 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 "MAY 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 SCF-relevant terminology:

- Adequate Security. A term describing protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized access to or modification of information.
- Artificial Intelligence and Autonomous Technologies (AI/ML). A term describing tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.
- Assessment Boundary. A term describing 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, Facilities and/or Artificial Intelligence (PPTDF-AI) 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. A term describing the item (e.g., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
- Assessment Objective (AO). A term describing objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.

[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*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- Asset. A term describing any data, device, application, service or other component of the environment that supports information-related activities. An asset is a resource with economic value that an organization owns or controls.
- Asset Custodian. A term describing a person or entity with the responsibility to assure that the assets are properly maintained, are used for the purposes intended and that information regarding the equipment is properly documented.
- Assurance. A term describing the grounds for justified confidence that a security, compliance and/or resilience claim has been or will be achieved.
- Cloud Computing. A term describing a technology infrastructure model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It also includes commercial offerings for:
  - Software-as-a-Service (SaaS);
  - Infrastructure-as-a-Service (IaaS); and
  - Platform-as-a-Service (PaaS).
- Compensating Control. A term describing alternative security, compliance and/or resilience controls implemented in lieu of the deficient control that provide equivalent or comparable protection. Compensating controls:
  - Include physical, administrative and/or technical safeguards or countermeasures employed by an organization in lieu of the deficient control; and
  - Reduce risk to the affected system(s), service(s), application(s), service(s), individual(s) and/or organization(s) in a manner that is equivalent to, or comparable to, the protection offered if the deficient control was operational and effective.
- Conflict of Interest (COI). A term describing situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.
- Conformity Assessment. A demonstration that specified requirements are fulfilled. To learn more about conformity assessments, NIST published Special Publication 2000-01, *ABC's of Conformity Assessment*, which serves as a worthwhile primer on the subject.[4]
- Continuous Monitoring. A term describing ongoing situational awareness activities to support organizational risk decisions.
- Control. A term describing any management, operational or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help an organization accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.
- Control Assurance Automation (CAA). A term describing the use of automated mechanisms to continuously or periodically validate that security, compliance and resilience controls are properly implemented, operating as intended and producing reliable evidence of effectiveness. CAA may:
  - Include automated control testing, configuration validation, evidence collection, exception detection and reporting to support ongoing assurance activities; and
  - Reduce reliance on manual assessment procedures.
- Control Inheritance: A term describing the situation in which a Technology Asset, Application and/or Service (TAAS) 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.
- Control Objective. A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align an organization with accepted due diligence and due care requirements.
- Controlled Unclassified Information (CUI). A term describing a type of information that requires safeguarding, or dissemination controls, pursuant to and consistent with applicable United States (US) law, regulations and US Government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act. While CUI is unclassified, it requires control to prevent the release of information that, if aggregated with other sources of information, could reveal exploitable information to adversaries.
- Cybersecurity / Information Security. A term that covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.
- Data. A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched or retrieved via electronic networks or other electronic data processing technologies.
- Data Controller. A term describing the data privacy stakeholder (or data privacy stakeholders) that determines the purposes and means for processing Personal Data (PD) other than natural persons who use data for personal purposes.

[4] *NIST SP 2000-1 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.2000-01.pdf*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- Data Principle. A term describing the natural person to whom the Personal Data (PD) relates.
- Data Processor. A term describing the data privacy stakeholder that processes Personal Data (PD) on behalf of and in accordance with the instructions of a PD controller.
- Discretionary Security Requirements (DSR). A term describing 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.
- Due Care. A term describing the standard of care where a reasonable person would exercise in the same situation or under similar circumstances. This standard of care is used in a tort action to determine whether a person was negligent.[5]
- Due Diligence. A term describing the level of reasonable care or attention expected to avoid liability.[6]
- Enclave. A term describing the distinct set of Technology Assets, Applications, Services and Data (TAASD) that operate in the same security domain and share the protection of a single, common, continuous security perimeter.
- Encryption. A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.
- Enduring Exception. A term describing a special circumstance or system where remediation and full compliance with a statutory, regulatory or other compliance-related requirement is not feasible.
- External Service Provider (ESP). A term describing 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)).
- Evidence Request List (ERL). A term describing a finite list of supporting evidence used in an audit or assessment.
- Federal Contract Information (FCI). A term describing a type of information that is not intended for public release. FCI is provided by, or generated for, the US Government under a contract to develop, or deliver, a product or service to the US Government. This does not include information provided by the US Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.
- Guidelines. A term describing recommended practices that are based on industry-recognized secure practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation or use.
- Information Assurance. A term describing the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.
- Information Technology (IT). A term describing the computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.
- Implemented Capability. A term describing the technical, administrative or physical mechanism that:
    - Currently exists in a production environment; and
    - Are capable of demonstrating conformity with applicable requirements.
- Least Privilege. A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.
- Loss. A negative impact from an incident that can be categorized as:
    - Productivity loss;
    - Data loss;
    - Financial loss; and/or
    - Reputation loss.
- 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.

[5] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_care*

[6] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_diligence*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- 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 Impact. A term describing the potential financial impact to an organization's business operations that has a significant, meaningful and measurable effect. The threshold for material impact is defined by an organization's executive leadership team.
- 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 term describing a deficiency, or a combination of deficiencies, in an organization's security, compliance and/or resilience controls (including coverage 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.
- Minimum Compliance Requirements (MCR). A term describing the 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.
- Maturity Level Criteria (MLC). A term describing the specific criteria for each maturity level to define reasonable staffing, technologies and processes to implement a desired level of maturity.
- Mechanism. A term describing a:
    - Process or system that is used to produce a particular result; or
    - Device or method for achieving a security-relevant purpose.
- Peripheral Device. A term describing any device that is controlled by and can communicate with a technology asset, including:
    - Input-output devices:
        - Mice;
        - Monitors;
        - Keyboards;
        - KVM switches;
        - Printers; and
        - Scanners; and
    - External storage devices.
- Personal Data (PD) /Personal Information (PI). A term describing any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

- Policy. A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.
- Procedure. A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.
- Process. A term describing the state when data is actively being used by a Technology Asset, Application and/or Service (TAAS) (e.g., accessed, entered, edited, manipulated, printed, viewed).
- Process Owner/Data Owner. A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, process or the data hosted on the asset or process. It does not mean that the asset belongs to the owner in a legal sense. Data/process owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained and used.
- Reciprocity. A term describing an agreement among participating organizations to accept each other's:
    - Security assessments to reuse system resources; and/or
    - Assessed security posture to share information.
- Resilience. A term describing the ability of People, Processes, Technologies and/or Facilities (PPTF) to anticipate, withstand, recover from and adapt to adverse conditions, disruptions or attacks while maintaining or rapidly restoring essential functions.
- Responsible, Accountable, Supportive, Consulted & Informed (RASCI). A term describing 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.
- 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: A term describing the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.
- Risk Tolerance: A term describing the level of risk an organization is willing to assume in order to achieve a potential desired result.
- Risk Threshold: A term describing the values used to establish concrete decision points and operational control limits to trigger management action and response escalation.
- Security. A term describing the condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.
- Security Control. A term describing administrative, physical and technical measures. These are safeguards, or countermeasures, prescribed for in-scope systems, applications, services, organizations, etc. to protect the Confidentiality, Integrity, Availability and Safety (CIAS) of an organization's data and systems.
- Sensitive Data. A term that covers categories of data that must be kept secure. Examples of sensitive/regulated data include sensitive Personal Data (sPD), Electronic Protected Health Information (ePHI) and all other forms of data classified as Restricted or Confidential.
- Sensitive Data Environment. A term that encompasses the People, Processes, Technologies, Data, Facilities & Artificial Intelligence (PPTDF-AI) that store, process and/or transmit sensitive/regulated data where. The Sensitive Data Environment (SDE) may be an enclave within the organization's existing IT infrastructure.
- Sensitive Personal Data (sPD)/Sensitive Personal Information (sPI). A term describing personal data, revealing:
    - The first name or first initial and last name, in combination with any one or more of the following data elements:
    - Social Security Number (SSN)/Taxpayer Identification Number (TIN)/National Identification Number (NIN);
    - Driver License (DL) or another government-issued identification number (e.g., passport, permanent resident card, etc.);
    - Financial account number; or

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- Payment card number (e.g., credit or debit card);
  - Racial or ethnic origin;
  - Political opinions;
  - Religious or philosophical beliefs;
  - Trade-union membership;
  - Physical or mental health;
  - Sex life and sexual orientation;
  - Genetic data; and/or
  - Biometric data.[7]
- Standard. A term describing formally established requirements in regard to processes, actions and configurations.
- Store. Storing is when data is inactive or at rest (e.g., located on electronic media, in system component memory or in physical format such as paper documents).
- Significant Change. A term describing change within, introduced into, or otherwise affecting the assessment boundary that materially alters the People, Processes, Technologies, Data, Facilities and/or Artificial Intelligence (PPTDF-AI), applicable requirements, control implementations, control inheritance, dependencies, or risk conditions upon which previous assurance was based.
- System. A term describing an asset; a system or network that can be defined, scoped and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls and mobile devices.
- Target Audience. A term describing the intended group for which a control or standard is directed.
- Threat. A threat:
  - Is a person, or thing, likely to cause damage or danger (noun); or
  - Indicates impending damage or danger (verb).
- Transmit. A term describing the state when data is being transferred/transmitted from one Technology Asset, Application and/or Service (TAAS) to another TAAS (e.g., data in transit using physical or digital transport methods).
- Trust. A term describing the belief that People, Processes, Technologies, Data, Facilities and/or Artificial Intelligence (PPTDF-AI) meet certain expectations and therefore, can be relied upon.

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 Services	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.
AI	Artificial Intelligence	Technology that performs tasks associated with human intelligence. In this guide, AI system data includes training and fine-tuning datasets, model weights, prompts, outputs, embeddings, vector stores and agent tool integrations.
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);

[7] *European Union General Data Protection Requirement – Article 9(1)*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

		▪ 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 Review	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: o Evaluate the legitimacy of the results from automated control assessments; and o Validate the automated evidence review process to derive a finding.
CASA	Continuous Assurance & Situational Awareness (CASA)	CASA allows third-party visibility of security, compliance and resilience control conformity and potential risk exposure.
CBOM	Cryptographic Bill of Materials	CBOMs are a structured record containing details about cryptographic assets used by a system, product, service or software component and the relationships and dependencies among those assets.
CAA	Control Assurance Automation	CAA is use of automated mechanisms to continuously or periodically validate that security, compliance and resilience controls are properly implemented, operating as intended and producing reliable evidence of effectiveness.
CDPAS	Cybersecurity & Data Protection Assessment Standards	A cohesive, consistent set of standards to govern cybersecurity and data protection related 3PAAC Services.
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.
CICA	Continuous Incremental Conformity Assessment (CICA)	CICA is an alternative to a point-in-time assessment that reflects the realities of continuous change within organizations. This approach utilizes an incremental assessment methodology, similar in concept to how incremental backups augment a full backup to provide an efficient way to ensure data is protected. This enables an organization to adopt a monthly, quarterly or annual assessment cadence that focuses on change. This model helps demonstrate an organization’s commitment to managing its ongoing compliance requirements.
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.
CSP	Cloud Service Provider	CSP refers to an external company that provides cloud services based on cloud computing. An External Service Provider (ESP) providing cloud computing services is a CSP. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is based on the definition for cloud computing in NIST SP 800-145. This cloud model is composed of five (5) essential characteristics, three (3) service models, and four (4) deployment models. Essential Characteristics:

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

		(1) On-demand self-service; (2) Broad network access; (3) Resource pooling; (4) Rapid elasticity; and (5) Measured service. Service Models: (1) Software as a Service (SaaS); (2) Platform as a Service (PaaS); and (3) Infrastructure as a Service (IaaS). Deployment Models: (1) Private cloud; (2) Community cloud; (3) Public cloud; and (4) Hybrid cloud.
CVC	Conformity Validation Cadence	CVC is a time-based criteria (e.g., monthly, quarterly, semi-annual, annual, etc.) to help OSAs determine the appropriate cadence to validate control operation and conformity.
DSR	Discretionary Security Requirements	DSR are discretionary cybersecurity and/or data protection 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)).
FD	Focal Document	FDs are laws, regulations and/or frameworks that are the target of crosswalk mapping exercises.
FDE	Focal Document Element	FDEs are the unique requirements within a FD (e.g., a specific requirement within a law, regulation or framework).
HBOM	Hardware Bill of Materials	HBOMs are a structured record containing details about physical components, assemblies, subassemblies and component parts that comprise a finished hardware product, together with relevant manufacturer, supplier, provenance and supply-chain relationship information.
HSC	Harvestable Sensitive Ciphertext	HSC is a term defined by this guide. It refers to sensitive/regulated data encrypted that: ▪ Uses a cryptographic mechanism whose future confidentiality depends on quantum-vulnerable public-key cryptography; and ▪ Whose required confidentiality lifetime may extend beyond the organization's expected Post Quantum Cryptography (PQC) migration period.
IC	Implemented Capability	IC refer to technical, administrative and physical controls where: ▪ Technology capabilities will only be considered implemented if the system(s), application(s) and/or service(s) has/have been operational in a production environment for at least sixty (60) days; ▪ Administrative processes will only be considered implemented if there is evidence to demonstrate that process has been: o Used in a real-world situation (e.g., onboarding/offboarding personnel, incident response, etc.); and/or

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

		○ Formally tested (e.g., documented incident response exercise); and ▪ Physical capabilities will only be considered implemented if the physical security mechanism(s) has/have been operational in a production environment for at least thirty (30) days.
ICS	Industrial Control Systems	ICS are a type of OT. An ICS is broader system of technologies that includes PLCs, sensors and networks.
IoT	Internet of Things	IoT refers to Internet-enabled technologies (e.g., smart devices) that can provide monitoring and automation tasks.
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.
ML	Machine Learning	ML is a subset of AI that enables systems to learn from large data sets to identify patterns and make predictions without being explicitly programmed for every specific task.
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.
MPIT	Manual Point In Time	MPIT is a traditional assessment methodology that: ▪ Is 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.
MSA	Master Services Agreement	MSAs are comprehensive contracts between two parties that establish terms and conditions of current and future transactions.
NPE	Non-Person Entity	An entity with a digital identity that acts in cyberspace but is not a human actor (e.g., devices, applications, service accounts, AI agents). The USG uses NPE consistent with NIST and DoD usage.
OSA	Organization Seeking Assessment	A company, entity or business unit seeking the external assessment.
OSC	Organization Seeking Certification	An OSC is an entity seeking to contract, obtain, or maintain certification. An OSC is also an OSA.
OT	Operational Technology	OT encompasses systems that detect and/or cause direct changes in the physical world by monitoring and controlling assets and processes (e.g., industrial technologies).
PaaS	Platform as a Service	PaaS is a cloud computing model that provides pre-configured tools, databases and middleware as a platform that enables consumers to build, deploy and manage applications. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
PbD	Privacy by Design	Data privacy through the design and governance of processes and technologies. PbD prioritizes data protection as a core business requirement, rather than a technical feature.
PLC	Programmable Logic Controller	PLCs are a type of IT. PLCs are "ruggedized" technologies that are designed for industrial settings to automate manufacturing processes, machineries and/or industrial systems.
PPTDF	People, Processes, Technologies, Data & Facilities	Five (5) components that provide a lens to view the applicability of controls: ▪ People - Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.). ▪ Processes - Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.). ▪ Technologies - Control directly applies to systems, applications and services (e.g., secure baseline configurations, patching, etc.). ▪ Data - Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.). ▪ Facilities - Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

PQC	Post-Quantum Cryptography	Refers to the development of cryptographic systems that are designed to stay safe and secure even against attacks from future, powerful quantum computers.
P/S/T	Process, Store and/or Transmit	Refers to processing, storing and/or transmitting data where: ▪ Store - Data is inactive or at rest (e.g., located on electronic media, in system component memory or in physical format such as paper documents). ▪ Process - Data is actively being used by a system component (e.g., accessed, entered, edited, manipulated, printed, viewed). ▪ Transmit - Data is being transferred/transmitted from one asset to another asset (e.g., data in transit using physical or digital transport methods).
QVC	Quantum-Vulnerable Cryptography	QVC is a term defined by this guide. It refers to cryptography whose security depends on mathematical problems (e.g., integer factorization, discrete logarithms) that a cryptographically relevant quantum computer is expected to solve.
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.
SBOM	Software Bill of Materials	SBOMs are a structured record containing details about the software components used to build or operate a software product and the supply-chain relationships among those components.
SCADA	Supervisory Control and Data Acquisition	SCADA is a type of OT. It is a Human-Machine Interface (HMI) for operators to monitor, control and adjust physical industrial processes in real-time.
SCF	Secure Controls Framework	A community driven metaframework that contains over 1,500 controls spanning over 200 cybersecurity and data privacy laws, regulations and frameworks.
SCR	Secure, Compliant & Resilient	Refers to the three (3) key components of the SCF's Secure, Compliant & Resilient Management System (SCRMS): Secure, Compliant & Resilient.
SOW	Statement of Work	SOWs are contracts that cover the work management aspects of a project (e.g., scope, timeline, cost, responsibilities, etc.).
SPD	Security Protection Data	SPD refers to security-relevant data that includes, but is not limited to: ▪ Configuration data; ▪ Event log files; ▪ Vulnerability data; and ▪ Authenticators (e.g., passwords).
TAAS	Technology Assets, Applications and/or Services	A term to cover technology assets, including systems, applications and services.
TAASD	Technology Assets, Applications, Services and/or Data	A term to cover technology assets, including systems, applications and services and that data that is stored, processed and/or transmitted by those technology assets.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

This guide is for educational purposes only. Users 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 security, compliance & resilience 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 security, compliance and resilience operations by simplifying the underlying controls that comprise the basis of an organization's security, compliance and resilience 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," that contains a catalog of controls made up of over 200 authoritative sources (e.g., statutory, regulatory and contractual frameworks). Additionally, this controls catalog contains over 1,500 controls and is logically organized into thirty-four (34) 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 security, compliance and resilience 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 an organization's needs. However, for companies that have two or more (2+) 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 security, compliance and resilience control frameworks.

In developing the SCF, we identified and analyzed over 200 security, compliance & resilience 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 1,500 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 1,500+ controls in the SCF. That is just not the case. It is best to visualize the SCF as a "buffet of security, compliance and resilience controls," where the presented buffet is a selection of 1,500+ 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 your organization, you can generate a customized control set that provides the controls needed to address your organization's security, compliance and resilience needs. The concept of tailoring the control set is explained at the end of this section.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Integrated Controls Management (ICM) Mindset

Cybersecurity is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization's security, compliance and resilience operations.

This affects the entity's overall business rhythm, since the controls used to define "secure practices" have both direct and indirect impacts on the Technology Assets, Applications, Services and/or Data (TAASD) that business operations rely upon.



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 security, compliance and resilience, 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 security, compliance and resilience 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 security, compliance and resilience compliance obligation that an organization faces.

The SCF is not:

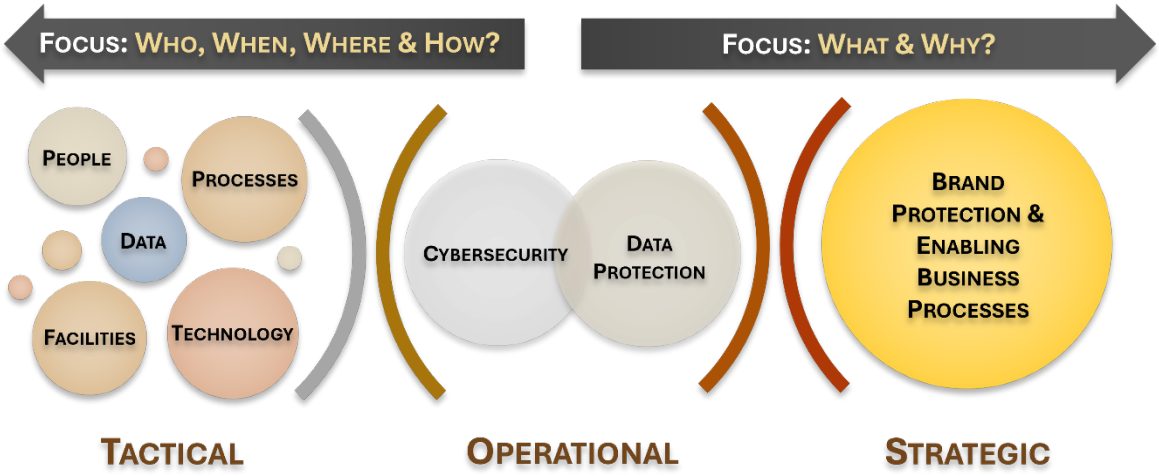
- A substitute for performing due diligence and due care to understand and manage an organization's specific compliance needs;
- A complete technology or documentation solution to address all security, compliance and resilience needs (e.g., the policies, standards, procedures and processes an organization needs to have in place to be secure and compliant); and
- Infallible or guaranteed. SCF controls are mapped based on expert-derived assessments to provide the control crosswalking that relies on human expertise and that is not infallible.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 security, compliance and resilience at the strategic, operational and tactical levels within an organization!



Using the SCF should be viewed as a long-term tool to not only help with compliance-related efforts but to ensure security, compliance and resilience principles are properly designed, implemented and maintained. The SCF helps implement a holistic approach to protecting the Confidentiality, Integrity, Availability and Safety (CIAS) of an organization's Technology Assets, Applications, Services and/or Data (TAASD). The SCF can be used to assist with strategic planning down to tactical needs that directly or indirectly impact People, Processes, Technologies, Data and/or Facilities (PPTDF).

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 3. 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 an organization invests in security, compliance and resilience 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 security, compliance and resilience practices are ignored. Regardless of the specific reason, those charged with developing, implementing and running an organization's security, compliance and resilience 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.[8]

Considering how business practices continuously evolve, so must cybersecurity practices. A 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 security, compliance and resilience capabilities work together to keep everything both secure and operational.

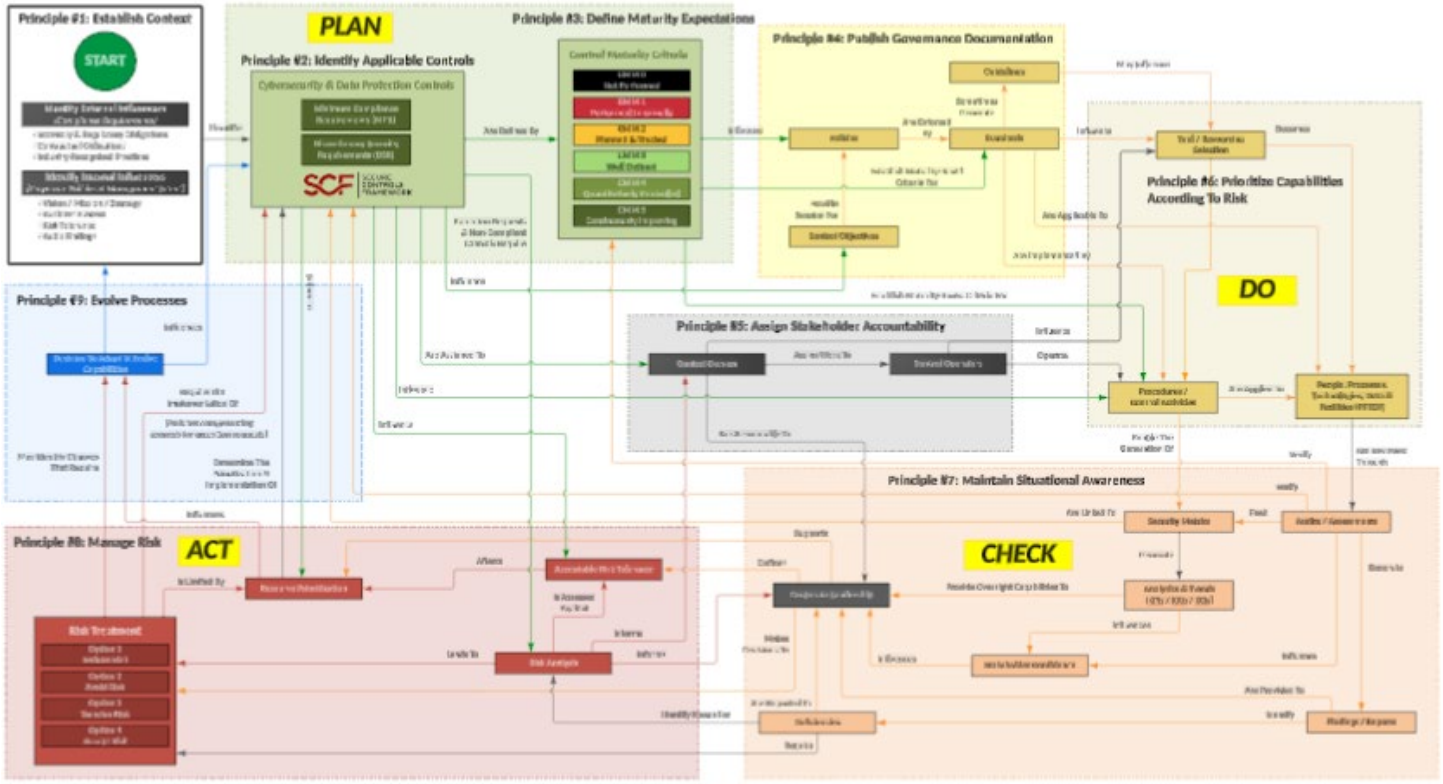
The PDCA approach is a logical way to conceptualize how GRC works:

- Plan. The overall process begins with planning. At its core, this phase is the process of conducting due diligence. The results of this process will define necessary controls (e.g., requirements) that influence the need for policies, standards and procedures. These actions directly influence resourcing and procurement actions that range from staffing needs to tool purchases and services acquisition.
- Do. This phase is the process of conducting due care, where it is focused on the "reasonable care" necessary to properly and sufficiently conduct operations that demonstrate the absence of negligence. This is the execution of procedures – the processes that bring controls to life.
- Check. This phase can be considered maintaining situational awareness. There are several ways to maintain situation awareness and that ranges from control validation testing to audits/assessments and metrics.
- Act. This phase again brings up the concept of "reasonable care" that necessitates taking action to maintain the organization's targeted risk tolerance threshold. This deals with addressing two main concepts (1) real deficiencies that currently exist and (2) areas of concern that may expose the organization to a threat if no action is taken.

[8] *PDCA approach to GRC - https://content.securecontrolsframework.com/pdf/scf-plan-do-check-act.pdf*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

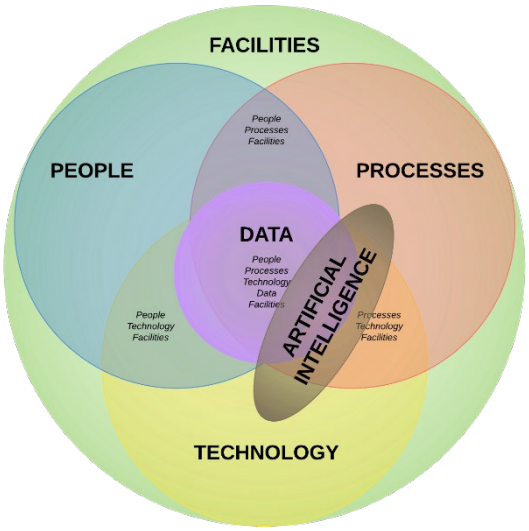


People, Processes, Technology, Data, Facilities and Artificial Intelligence (PPTDF-AI)

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

The PPTDF-AI model provides a comprehensive approach to address control applicability. These six (6) 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.).
6. Artificial Intelligence (AI) – Applicable to AI and autonomous technologies – applies across technologies, processes and data.



The premise is that controls are central to security, compliance and resilience operations as well as the business rhythms of the organization. Without properly defining minimum capability thresholds, an organization's overall security, compliance and resilience 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" enhances risk management discussions.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

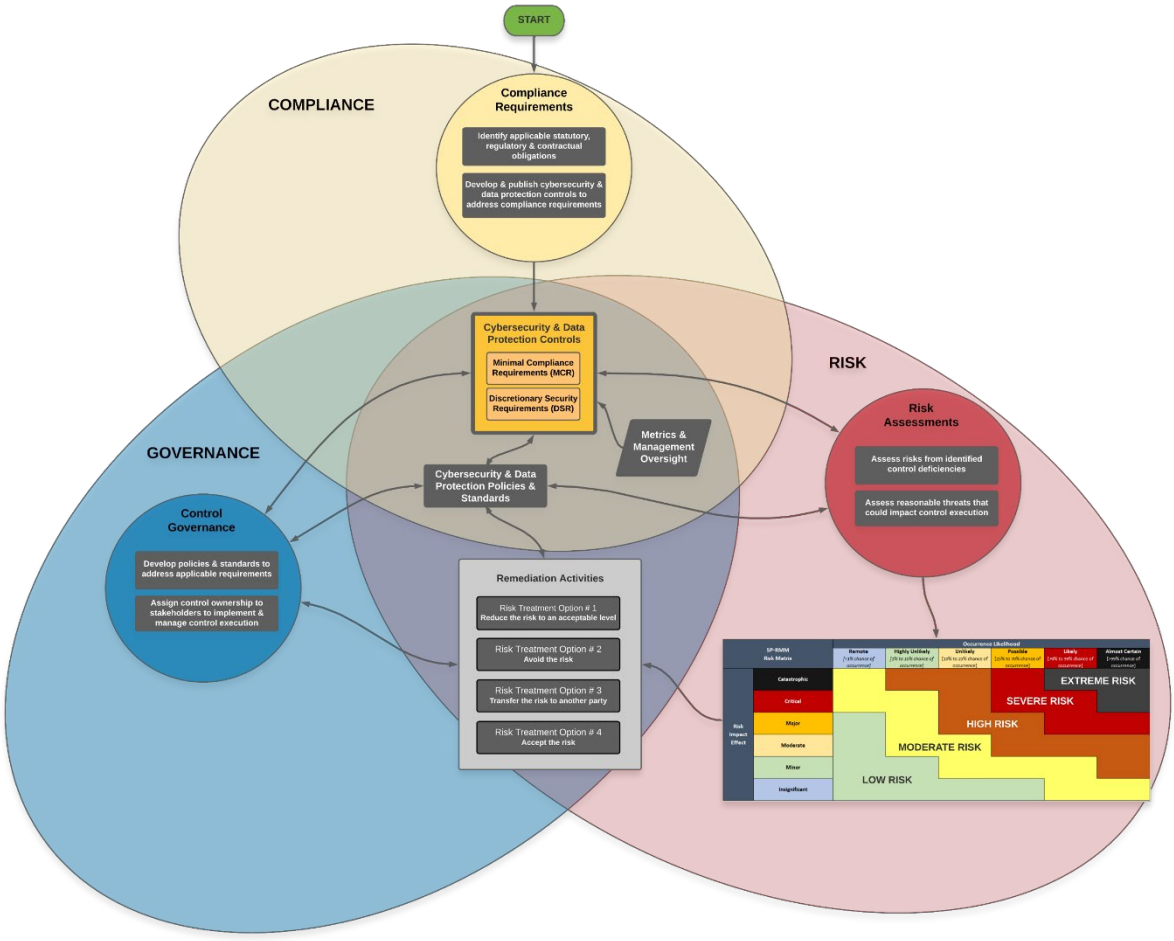
This guide is for educational purposes only. Users are encouraged to work with a competent professional to validate any compliance-related assumptions.

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.[9] 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 "chicken vs egg" debate with GRC functions. The following diagram shows the interrelated nature of governance, risk management and compliance functions.[10]



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 security, compliance and resilience perspective. This process involves interfacing with various Lines of Business (LOB) to understand how the organization operates, including geographic considerations. Generally,

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

[10] *GRC Component Relationships Diagram - https://content.securecontrolsframework.com/pdf/scf-grc-fundamentals.pdf*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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).

Compliance defines the controls necessary to meet the organization's specific needs (e.g., security, compliance and resilience) 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 security, compliance and resilience controls is necessary to ensure the results of risk assessments accurately 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:

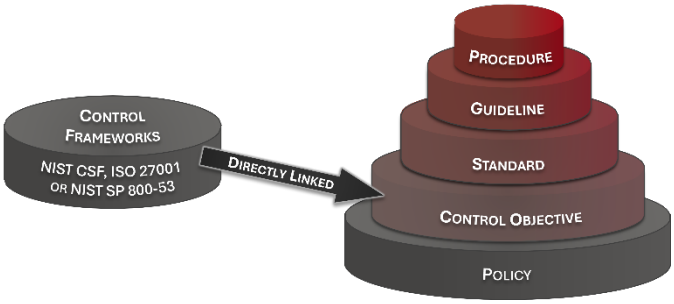
1. Develop policies and standards to meet those compliance obligations (defined by applicable control objectives); and
2. Assign ownership of those controls to the applicable stakeholders involved in the affected business processes. This process often requires a documented Responsibility, Accountability, 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 security, compliance and resilience 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 security, compliance and resilience 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.

Security, compliance and resilience documentation is generally comprised of six (6) main parts:

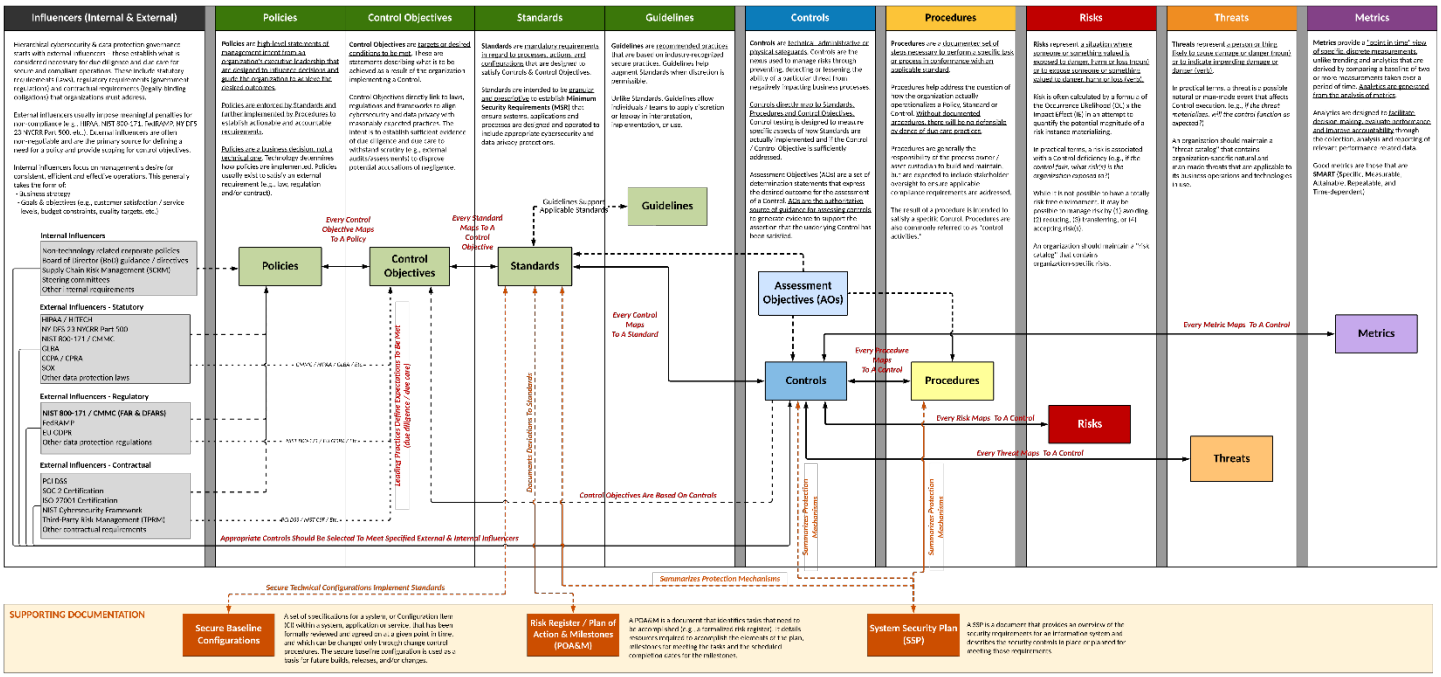
1. Policies establish management's intent;
2. Control Objectives identifies leading practices;
3. Standards provide quantifiable requirements;
4. Controls identify desired conditions that are expected to be met;
5. Procedures / Control Activities establish how tasks are performed to meet the requirements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



© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Governance documentation should be viewed from a hierarchical perspective and the Hierarchical Cybersecurity Governance Framework (HCGF) is an excellent way to visualize the interactions between various governance documentation components, based on industry-recognized definitions for policies, standards, procedures, etc.[11]



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 security, compliance and resilience 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.

[11] *Hierarchical Cybersecurity Governance Framework (HCGF) - https://content.complianceforge.com/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Section 4. Control Weighting, Tailoring & Compensating Controls

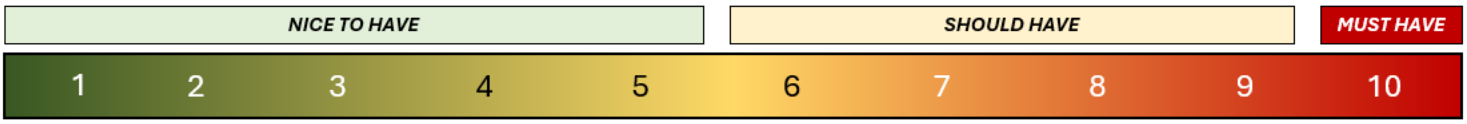
This section focuses on three (3) of the most common questions pertaining to getting started with the SCF:

1. Control weighting;
2. How to tailor the SCF control set; and
3. Compensating controls.

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:*[12]

- *≥ 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 Controls Are Applicable

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 organization's 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 an 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 an organization's specific needs!

Understanding the requirements for both security, compliance and resilience 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.

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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.

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 security, compliance and resilience 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 security, compliance and resilience 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

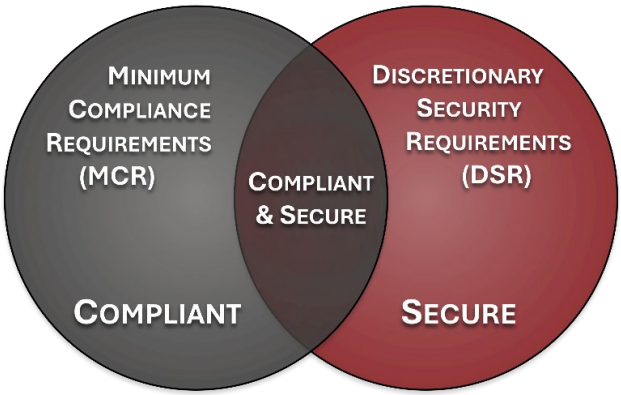
From a security, compliance and resilience perspective, common contractual compliance examples include but are not limited to:

- 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)

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:

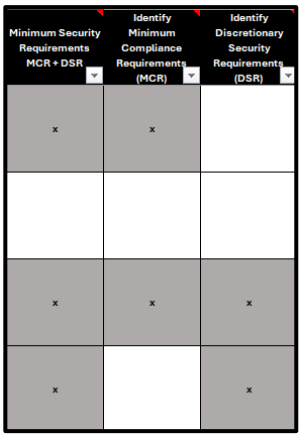
- Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure 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 security, compliance and resilience 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.



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. 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.



© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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.

Compensating Controls

Compensating controls are a reality for organizations and must be proactively managed. The lifespan for a compensating control may be short (ideal scenario) or it may be a part of a long-term risk mitigation strategy (e.g., will not get remediated until the next hardware refresh that may be several years in the future).

Compensating controls are not a "shortcut" to bypass unmet requirements, since the use of compensating controls is:

- Part of a deliberate, defensible risk treatment methodology that is used when a primary control cannot be implemented as prescribed; and
- Focused on matching the primary control's objective and outcome.

A compensating control is an alternative control (or set of controls) that provides equivalent or comparable risk mitigation when the implementation of the primary control is:

- Technically infeasible;
- Operationally impractical;
- Cost-prohibitive; and/or
- Temporarily unavailable (e.g., phased implementation where the primary control is planned, but not yet implemented).

For clarity purposes, it is important to separate these similar, yet distinctly different, concepts:

- Compensating controls are ALTERNATIVE implementations of the control to achieve equivalent protection; and
- Control enhancements are ADDITIONAL safeguards beyond the baseline control set.

Without this separation, users may blur these lines, which can create legal exposure. Most laws, regulations and frameworks have allowances for compensating controls, but do not provide guidance on how to select and/or operationalize them. The SCF provides structured, risk-aligned guidance to support defensible implementation of compensating controls.

Scenarios where compensating controls would be considered acceptable include, but are not limited to:

- Legacy systems that cannot support modern controls (e.g., antimalware, FIM, etc.);
- Regulatory conflicts (e.g., cryptographic module requirements);
- Technology limitations (e.g., inability to patch embedded software components); and
- Interim risk treatment during remediation actions.

Scenarios where compensating controls would be considered unacceptable include, but are not limited to:

- Avoiding cost or effort without legitimate justification (e.g., able to withstand external scrutiny);
- Lack of sufficient management level for risk acceptance (e.g., violates risk appetite); and
- Alternative controls that are not appropriate (e.g., do not provide equivalent or comparable risk mitigation).

Compensating Control Considerations

There may be technical and/or business limitations that impact an organization's ability to implement a primary control. That is when a compensating control would be evaluated to be added to the Living Control Set (LCS) as a control to mitigate the risk(s) associated with the non-existent or deficient primary control.

The concept of the LCS defines "what good looks like right now" for an organization. The LCS is meant to evolve over time as requirements evolve and the organization's maturity improves. Compensating controls are important since they play a part in the LCS, where compensating controls:

- Can be used when primary implementations are not feasible; and
- Are expected be tied to evidence artifacts to keep everything grounded in defensible implementation.

Technical limitations may prevent a primary control from being implemented. Examples include, but are not limited to:

- A specialized system is incapable of having antimalware or host-based firewall software installed;
- An antiquated system is not capable of being patched, since it is unsupported; and

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- A new patch is not certified for a certain operating environment and cannot be applied until approved by the OEM.

Business limitations may prevent a primary control from being implemented. Examples include, but are not limited to:

- A contract exists that prevents changes to an operating environment until approved by an outside partner (e.g., partner);
- Service Level Agreements (SLA) for downtime affect certain environments from being patched at the same cadence as the rest of the organization; and
- Remote workforce limitations for implementing physical security controls for logical and/or physical access.

What Compensating Controls Are

Compensating controls are security, compliance and/or resilience controls that an organization may employ in lieu of the primary control (e.g., a control from the organization's baseline control set) that provide equivalent or comparable protection to the People, Process, Technology, Data and/or Facility (PPTDF). [13]

What Compensating Controls Are Not

It is important to clarify a few points about what compensating controls are not:

- Compensating controls are not: *"If you can't do control HRS-03, here are XYZ alternatives."* That is a dangerous mindset.
- Risk acceptance is not a compensating control – it is a LEADERSHIP DECISION.

It is vitally important for compensating controls to be assessed for:

- Applicability;
- Risk mitigation; and
- Sustainability.

Proposed compensating controls are expected to be evaluated by an organization's leadership, since accepting risk associated with a compensating control is a leadership decision. Risk evaluation is expected to be formalized where documentation should exist to capture:

- Available alternatives;
- Justification for the selected compensating controls; and
- If applicable, follow-up steps to validate the effectiveness of the compensating control.

Materiality Considerations For Compensating Controls

There is a "materiality ecosystem" that exists within modern cybersecurity risk management discussions. The process begins with determining what constitutes materiality for an organization. This is organization-specific and is primarily based on a clearly-defined financial threshold.

The SCF Council defines the materiality threshold for an organization's security, compliance and resilience program as, "A deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance."

Defining materiality is an executive leadership determination, not a cybersecurity determination. Often, cybersecurity teams incorrectly hypothesize what "should be material" through the myopic perspective of the cybersecurity department. However, those cybersecurity-led definitions are often incorrect and are not material to the organization, much to the frustration of legal counsel that sometimes have to reprimand cybersecurity practitioners for incorrectly labeling incidents as material. For example, while a $5 million dollar incident may appear material (e.g., it is a significant sum), that financial amount may not come close to the actual materiality threshold for a prosperous organization.

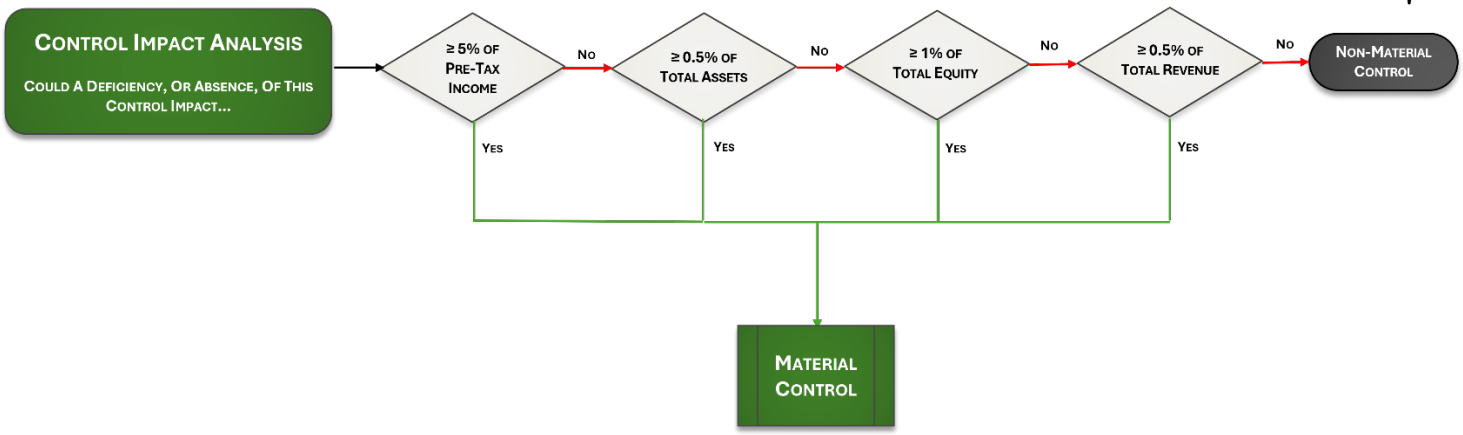
When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data protection control that:

- 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.

[13] *NIST Glossary for Compensating Controls - https://csrc.nist.gov/glossary/term/compensating_controls*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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



© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 5. DESIGNING & BUILDING AN AUDIT-READY CYBERSECURITY PROGRAM

Building an audit-ready security, compliance and resilience program requires addressing the holistic nature of security, compliance and resilience concerning how People, Processes, Technologies, Data & Facilities (PPTDF-AI) 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.

Security, compliance and resilience 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 security, compliance and resilience principles are designed, implemented and managed by default!

HOLISTIC APPROACH TO ADDRESS CONTROL APPLICABILITY

Cybersecurity practitioners generally agree that the importance of robust security, compliance & resilience 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 disparate laws, regulations and frameworks. With the publishing of NIST IR 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings,* it establishes the US Government's playbook for how to perform crosswalk mapping between different security, compliance & resilience-related 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]

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

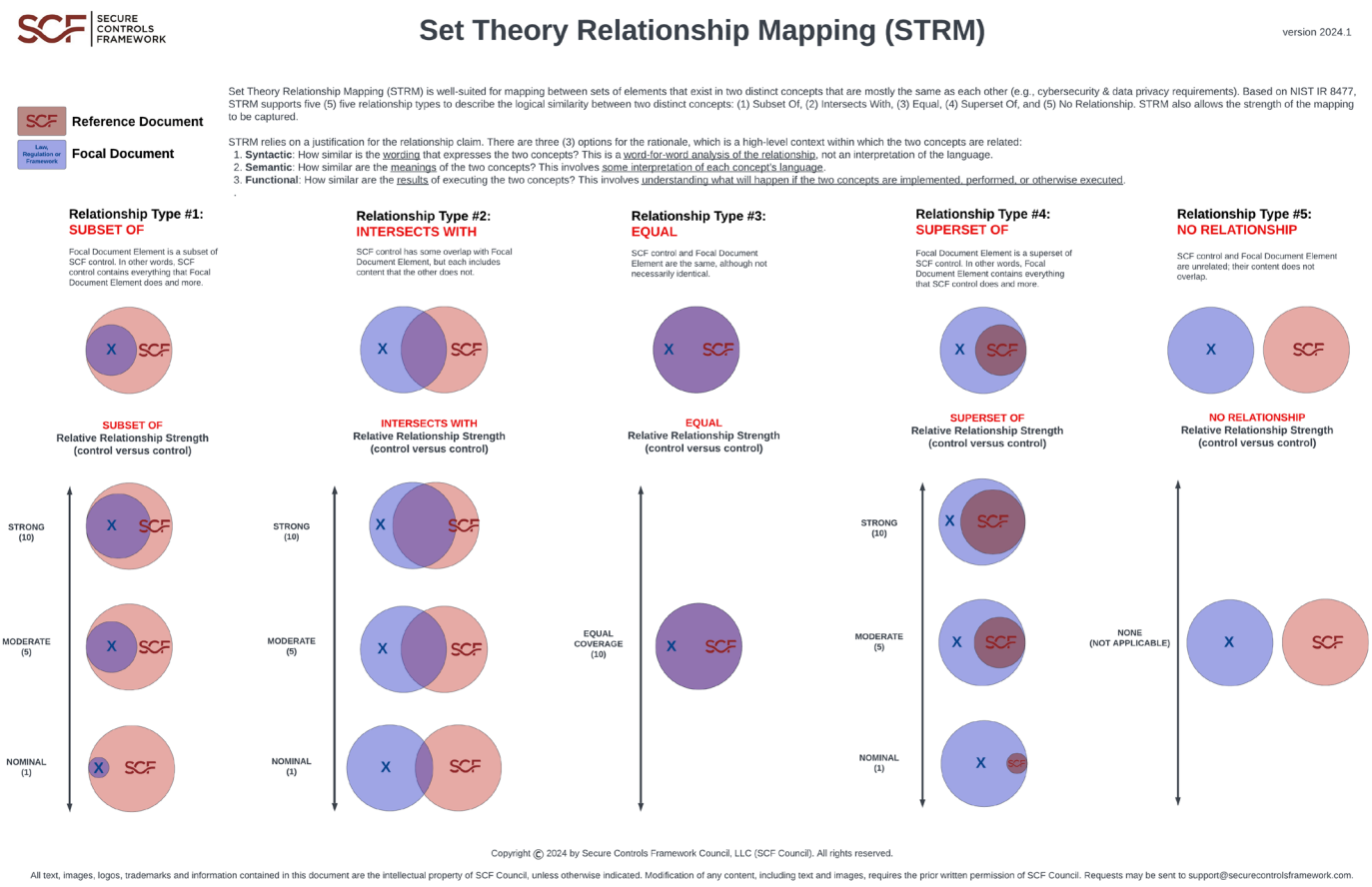
© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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." This can be visualized in the diagram shown below:[16]

REFERENCE DOCUMENT (RD)

FOCAL DOCUMENT (FD)



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.

[16] *SCF STRM mapping example - https://content.securecontrolsframework.com/pdf/scf-set-theory-relationship-mapping.pdf*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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.[17] 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.

[17] *37 CFR Part 202 - https://www.federalregister.gov/documents/2023/03/16/2023-05321/copyright-registration-guidance-works-containing-material-generated-by-artificial-intelligence*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 6. SECURE, COMPLIANT & RESILIENT MANAGEMENT SYSTEM (SCRMS)

The premise of Security, Compliance & Resilient Management System (SCRMS) is that controls are central to security, compliance and resilience 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),[18] 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 security, compliance and resilience 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."*

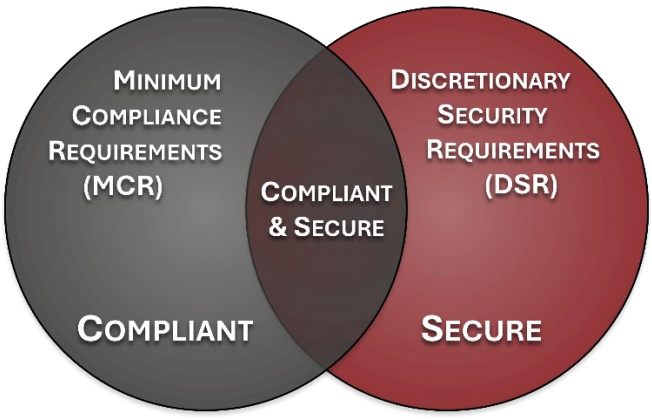
SCRMS takes a different approach from the traditional definition of Governance, Risk Management and Compliance (GRC) and/or Integrated Risk Management (IRM), since SCRMS is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization's security, compliance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

SCRMS is designed to proactively address the strategic, operational and tactical nature of operating an organization's security, compliance and resilience 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 security, compliance and resilience 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.



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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

IT General Controls (ITGC)

The combination of MCR and DSR equate to an entity's Minimum Security Requirements (MSR), which define the "must have" and "nice to have" requirements in one control set. This control set defines the Minimum Viable Product (MVP) technical and business requirements from a security, compliance & resilience perspective.

The MSR can be considered to be an entity's IT General Controls (ITGC), which establishes the necessary controls that must be applied to applicable Technology Assets, Applications, Services and/or Data (TAASD).

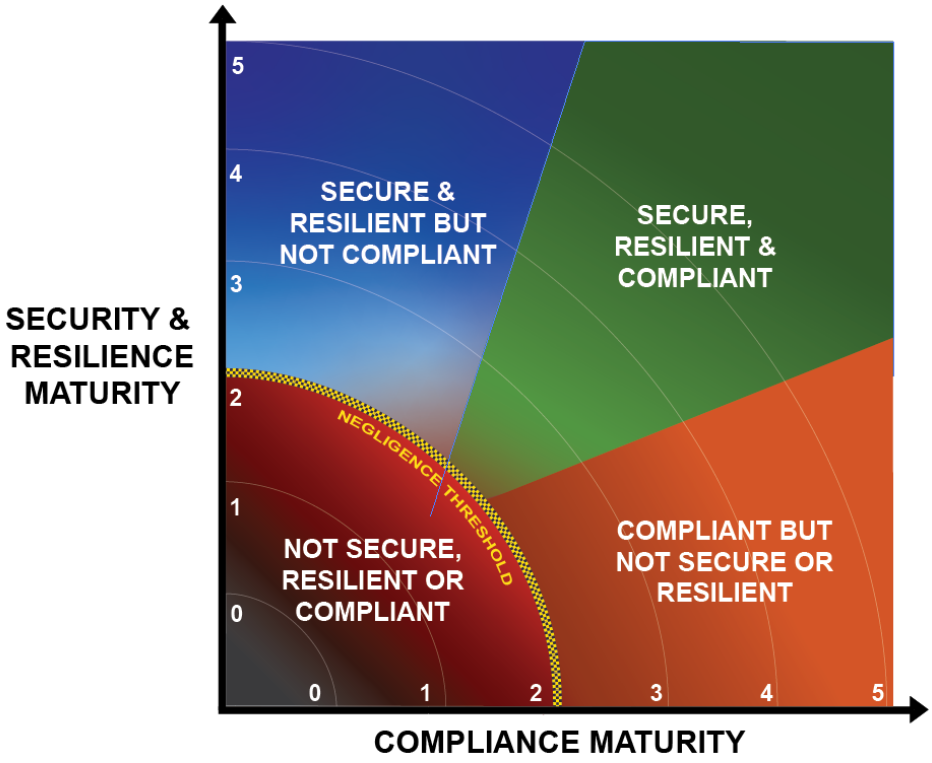
Security vs Compliance

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.

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?"*



This concept of identifying a negligence threshold is addressed in the SCF's Secure, Compliant & Resilient Capability Maturity Model (SCR-CMM).[19]

[19] *SCF C|P-CMM - https://securecontrolsframework.com/free-content/capability-maturity-model-scr-cmm/*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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);
- 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.[20]

NICE TO HAVE CONTROLS - Defining "Being Secure & Resilient" That Is Specific To Your Business Processes

Security, compliance & resilience 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 Security 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."*[21] From a discretionary control perspective, this may require the addition of technologies and processes to help ensure the continuity of business operations, such as:

[20] *Unified Scoping Guide - https://complianceforge.com/content/pdf/unified-scoping-guide-usg.pdf*
[21] *NIST Glossary - https://csrc.nist.gov/glossary/term/resilience#*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- 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.

Defining Negligence As It Pertains To Security, compliance and resilience

The following content is leveraged from Cornell's Law School Legal Information Institute (LII)[22] 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 whether the defendant has breached a duty, courts will usually use the *Learned Hand formula*[23], 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.

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

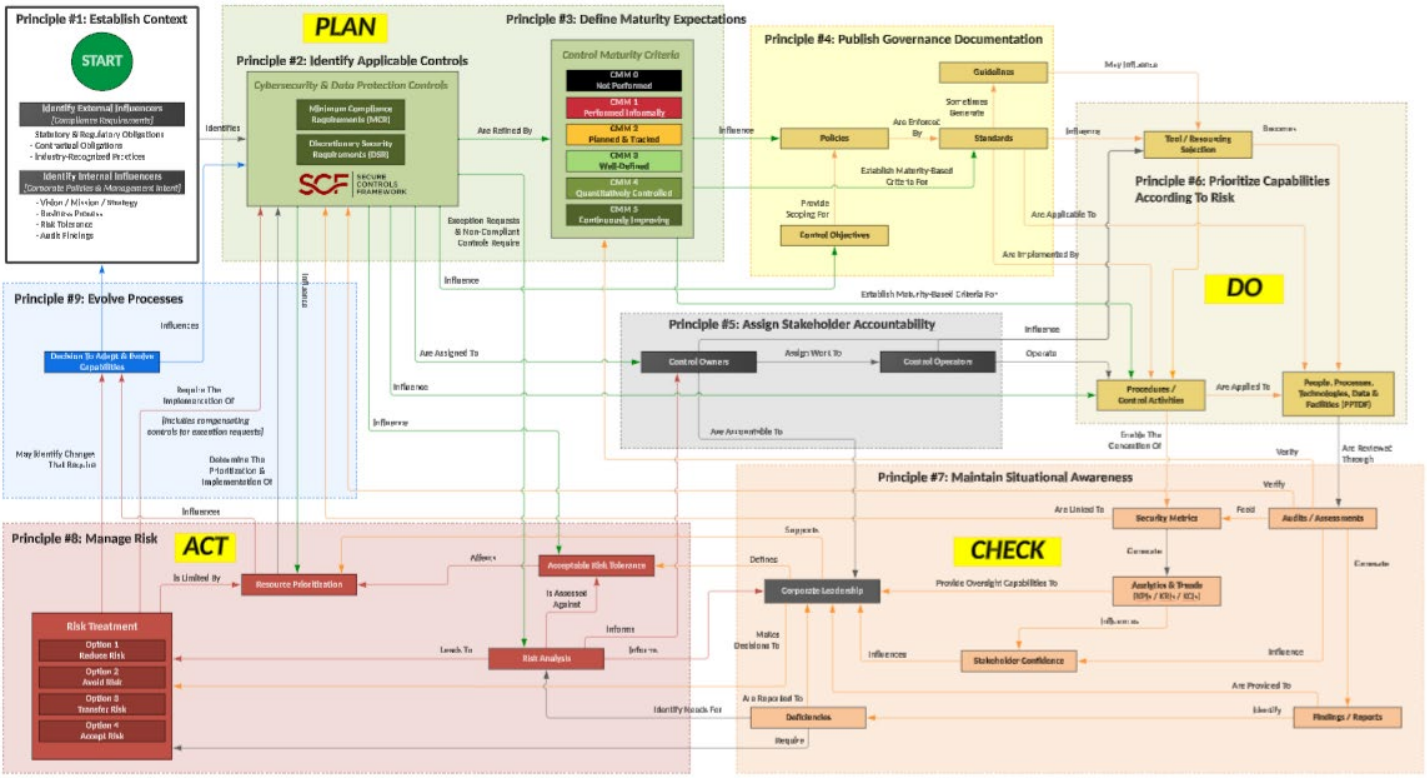
This guide is for educational purposes only. Users are encouraged to work with a competent professional to validate any compliance-related assumptions.

SCRMS Principles

There are nine (9) principles associated with the Secure, Compliant & Resilient 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; and
(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.



[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 security, compliance & resilience 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;

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- 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:
- *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 security, compliance & resilience 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.

SCF Council Guidance

Part of an entity's due diligence process is to identify applicable security, compliance & resilience controls. Practical steps to identify applicable controls include:

(1) Reading through the Secure Controls Framework (SCF) principles to become familiar with the thirty-four (34) domains to understand how they come together to address the security, compliance and resilience considerations for a modern security, compliance & resilience 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 security, compliance & resilience 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

There is no expectation for an entity to utilize all 1,500+ controls in the SCF catalog. It is best to visualize the SCF as a "buffet of security, compliance & resilience 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 security, compliance & resilience 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-AI).

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 Secure, Compliant & Resilient 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-AI 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

Security, compliance & resilience 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 security, compliance & resilience 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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

There are generally three (3) options to generate security, compliance & resilience 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 security, compliance and resilience 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's security, compliance & resilience capabilities. 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 security, compliance & resilience-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,

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 security, compliance & resilience 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 Secure, Compliant & Resilient 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 security, compliance & resilience 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

Security, compliance & resilience 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-AI.

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

(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 security, compliance & resilience 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.*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 7. SECURE, COMPLIANT & RESILIENT CAPABILITY MATURITY MODEL (SCR-CMM)

The SCR-CMM is meant to solve the problem of objectivity in both establishing and evaluating security, compliance and resilience 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 security, compliance and resilience 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 security, compliance and resilience 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 security, compliance and resilience 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

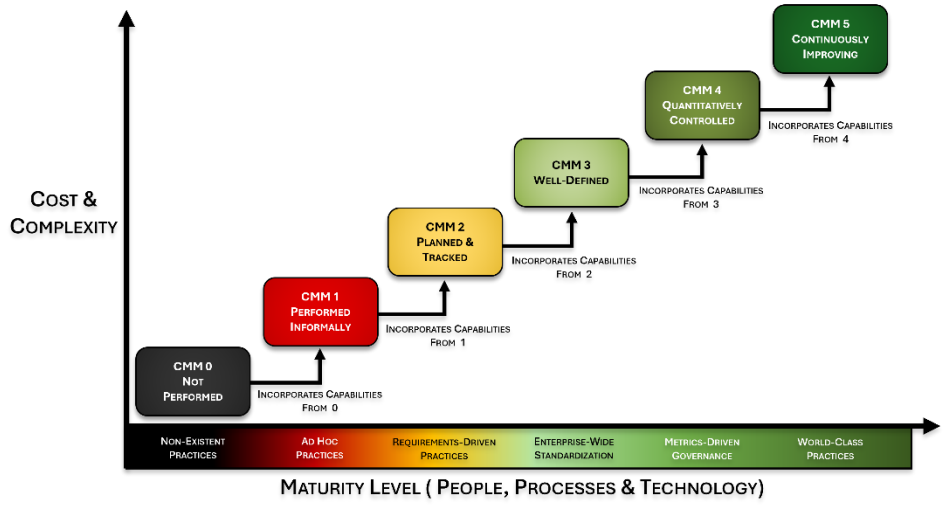
There are many competing models that exist to demonstrate maturity. Given the available choices, the SCF decided to leverage an existing framework, rather than reinvent the wheel. In simple terms, we provided control-level criteria to an existing CMM model.

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-AI 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).[24]

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)*.[25]

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.



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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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."*[26]

This stance on fraudulent misrepresentations may appear harsh, but it accurately describes the situation. There is no room in security, compliance & resilience 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 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."*[27] Increased rigor in control testing is what leads to increased assurance. Therefore, increased rigor and increased assurance are mutually inclusive.

The SCR Conformity Assessment Program (SCR CAP) leverages (3) three levels of rigor. The SCR 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:[28]

- **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 is 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

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

6. CMM Level 5 – Continuously Improving.

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[29] and due diligence[30] 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.

---

[29] *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.*

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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.*

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 security, compliance & resilience program so that it meets business objectives). Control or domain-specific CONOPS may be incorporated as part of a broader operational plan for the security, compliance and resilience 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.)*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- *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 security, compliance and resilience 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 security, compliance and resilience program (e.g., quarterly business reviews to the CIO/CEO/board of directors). This situational awareness is made possible*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

through detailed metrics.

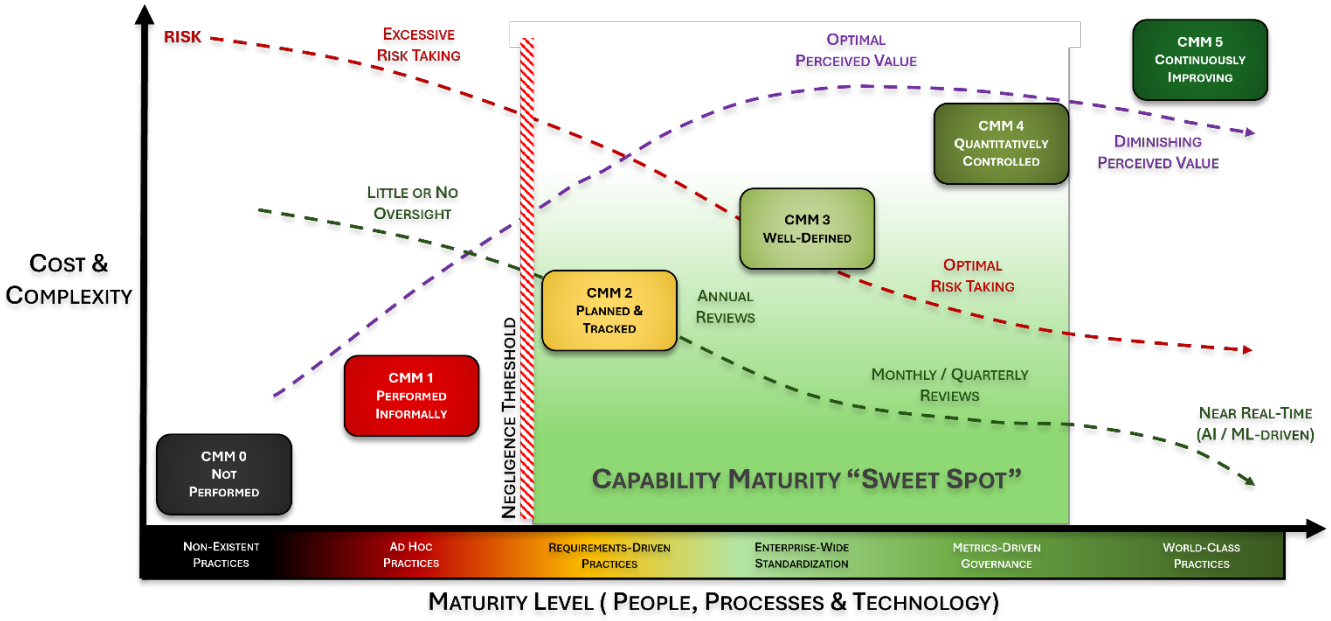
- *The organization has a very aggressive business model that requires not only IT, but its security, compliance and resilience practices, to be innovative to the point of leading the industry in how its products and services are designed, built or delivered.*
- *The organization invests heavily into 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 security, compliance and resilience 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 security, compliance and resilience 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 security, compliance and resilience 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, security, compliance and resilience. 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 security, compliance and resilience 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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).

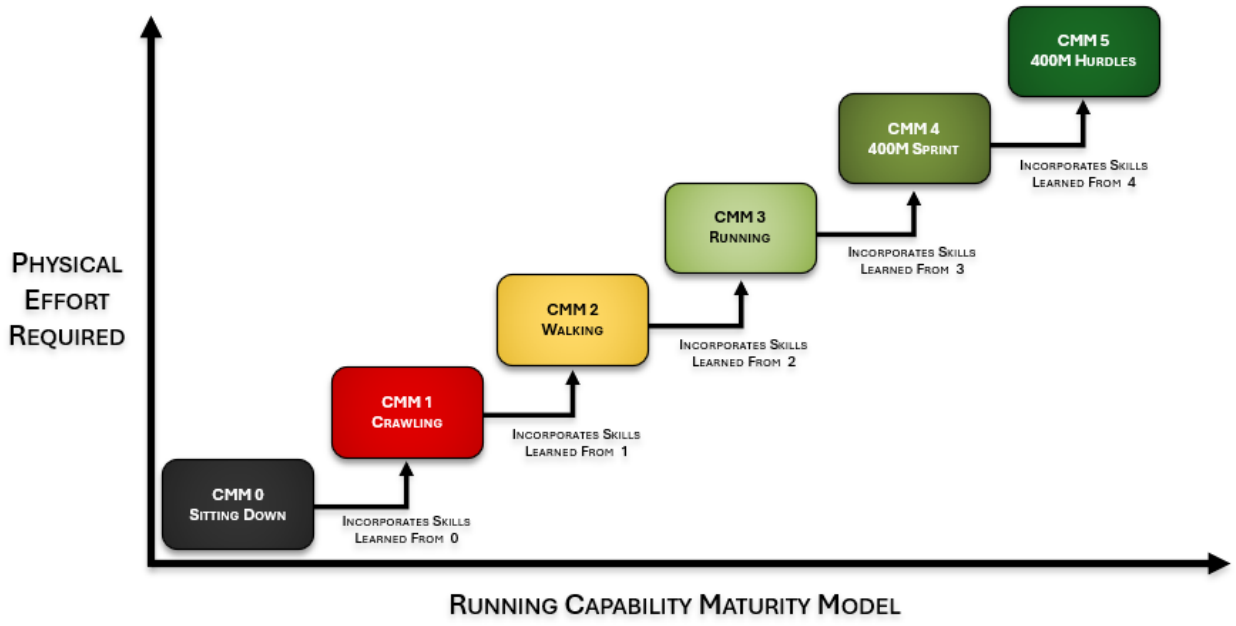
Stakeholder Value Considerations

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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- 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

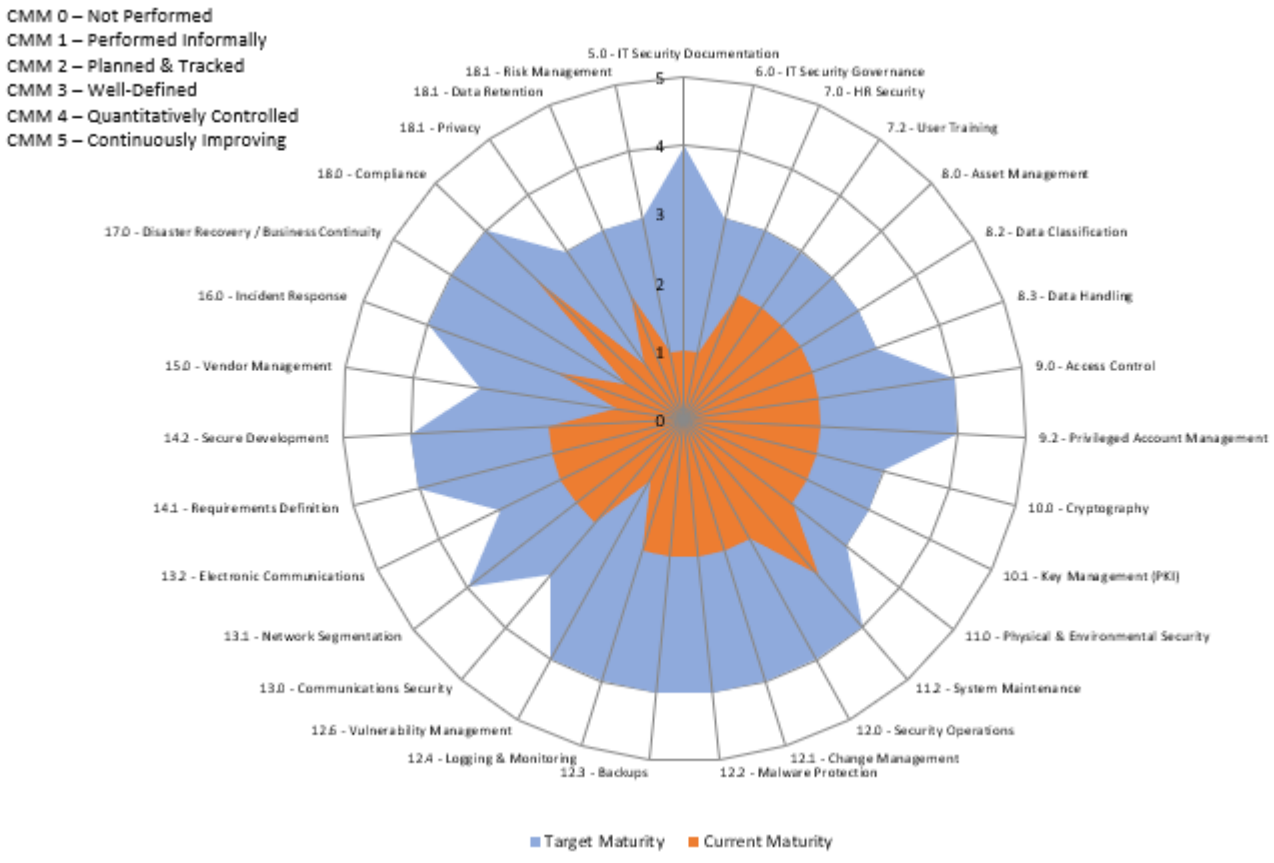
The SCR-CMM is meant to solve the problem of objectivity in both establishing and evaluating security, compliance and resilience controls. There are four (4) main objectives for the SCR-CMM:

1. Provide CISO/CPOs/CIOs with objective criteria that can be used to establish expectations for a security, compliance and resilience 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 security, compliance and resilience 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 security, compliance and resilience 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.



© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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-AI 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 security, compliance and resilience program, when, in reality, the department is an array of disjointed capabilities that lack 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-four (34) 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 security, compliance and resilience 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 security, compliance & resilience 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

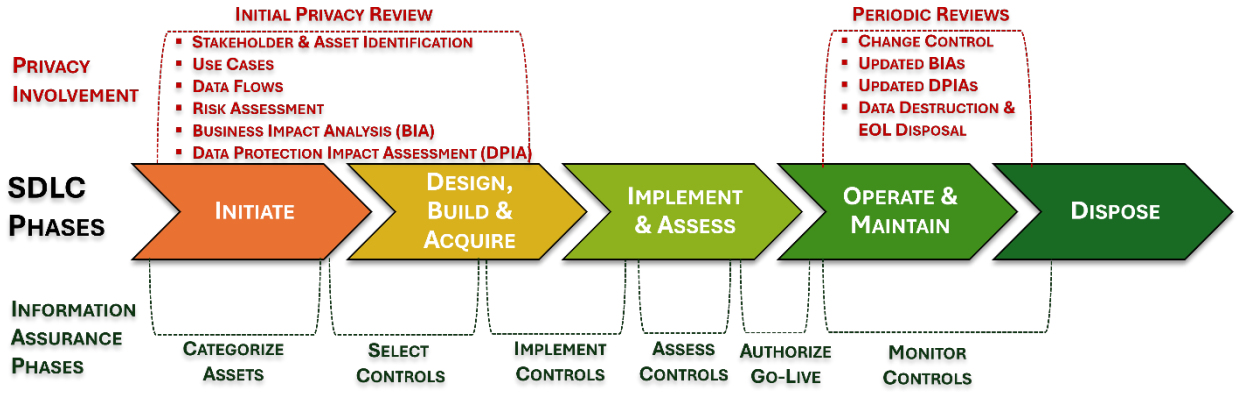
Referencing back to the SCR-CMM Overview section of this document, L0-1 levels of maturity are identified as being deficient

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 1,500 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 security, compliance and resilience controls. This necessitates oversight of ESPs to ensure controls are properly implemented and managed.

Identifying The Problem

In managing a security, compliance and resilience 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

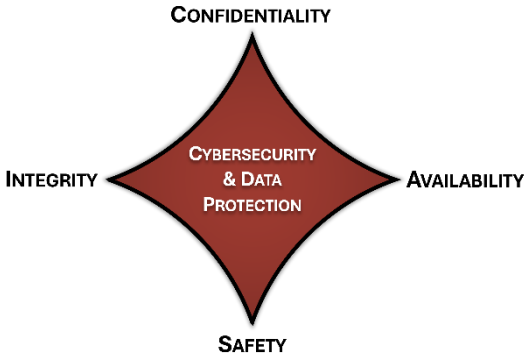
Referencing back to the SCR-CMM Overview section of this document, L0-1 levels of maturity are identified as being deficient from a "reasonable person perspective" in most cases. Therefore, organizations need to look at the "capability maturity sweet

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 security, compliance and resilience 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 1,500 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 security, compliance and resilience 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 security, compliance and resilience practices. That is why the SCF-B is a bespoke set of security, compliance and resilience controls that was purposely built for M&A to provide as complete a

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

picture as possible about the divesting entity's security, compliance and resilience 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 8. 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 security, compliance and resilience 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 security, compliance and resilience 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 security, compliance and resilience 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, procedures, evidence artifacts and assessment objectives all 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 security, compliance and resilience 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 security, compliance and resilience 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 security, compliance and resilience-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 security, compliance and resilience 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 security, compliance and resilience 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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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);
- Focus 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.).

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

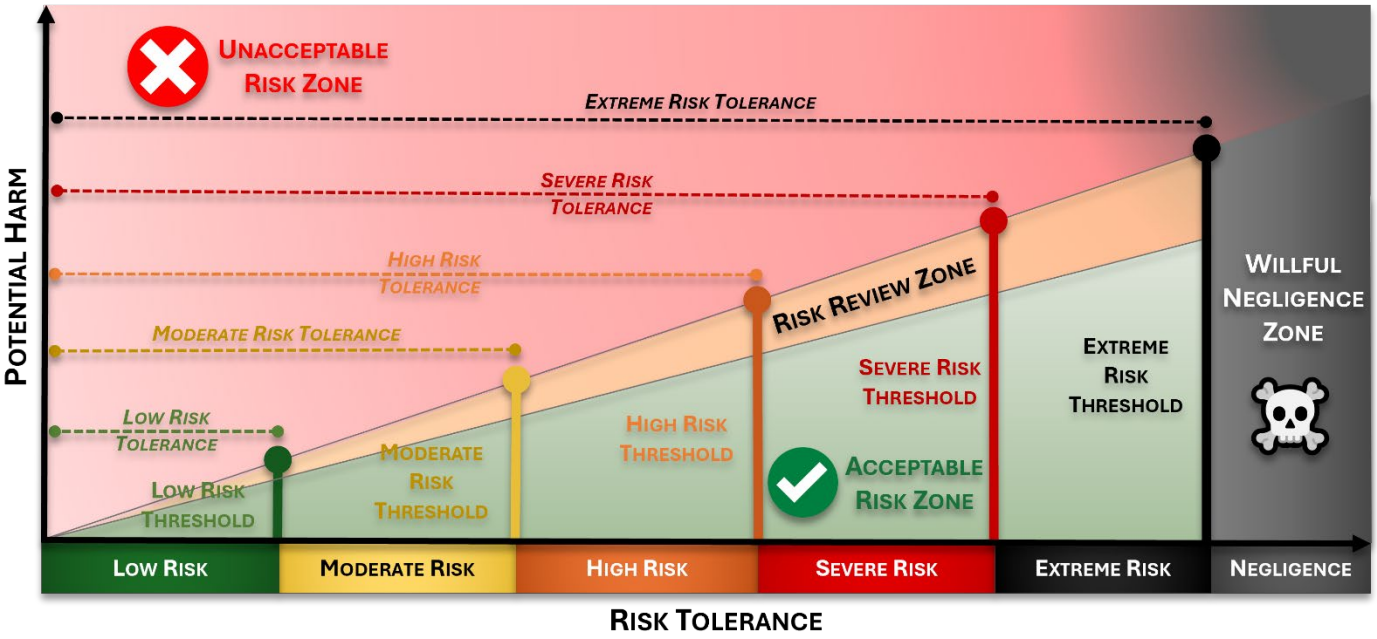
This guide is for educational purposes only. Users are encouraged to work with a competent professional to validate any compliance-related assumptions.

Baselining Risk Management Terminology

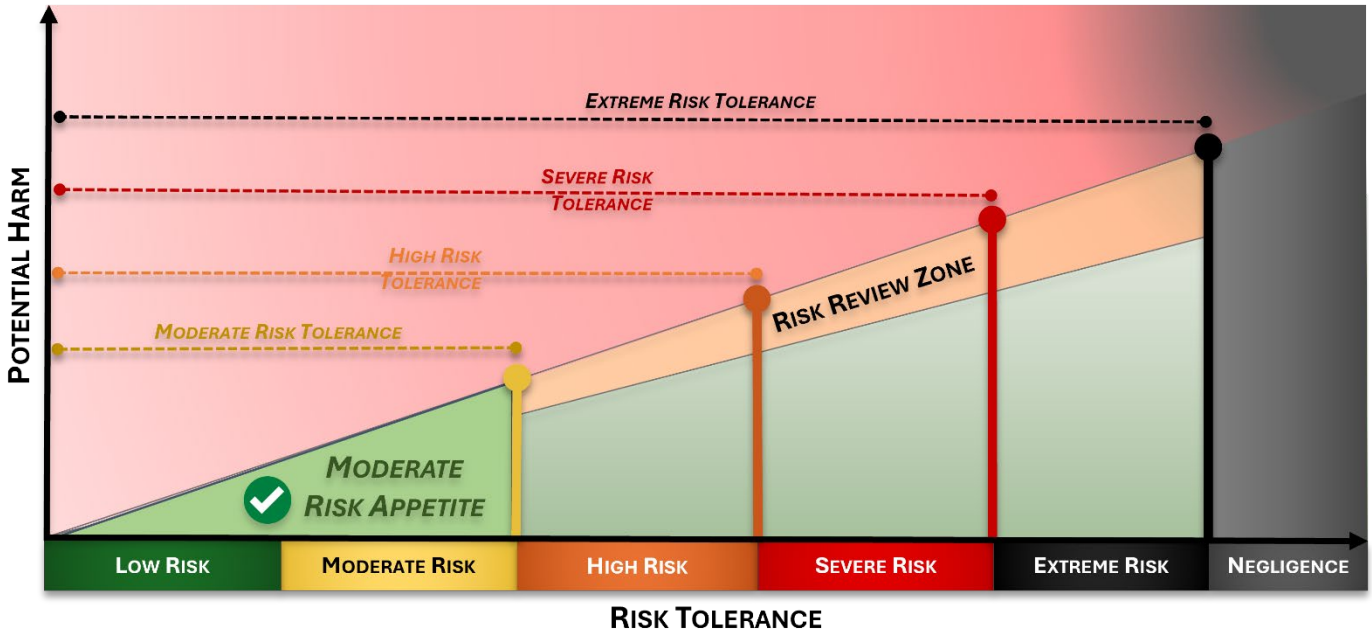
Risk management involves coordinated activities that optimize the management of potential opportunities and adverse effects. Proactive risk management activities provide a way to realize potential opportunities without exposing an organization to unnecessary peril.

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.



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:



© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

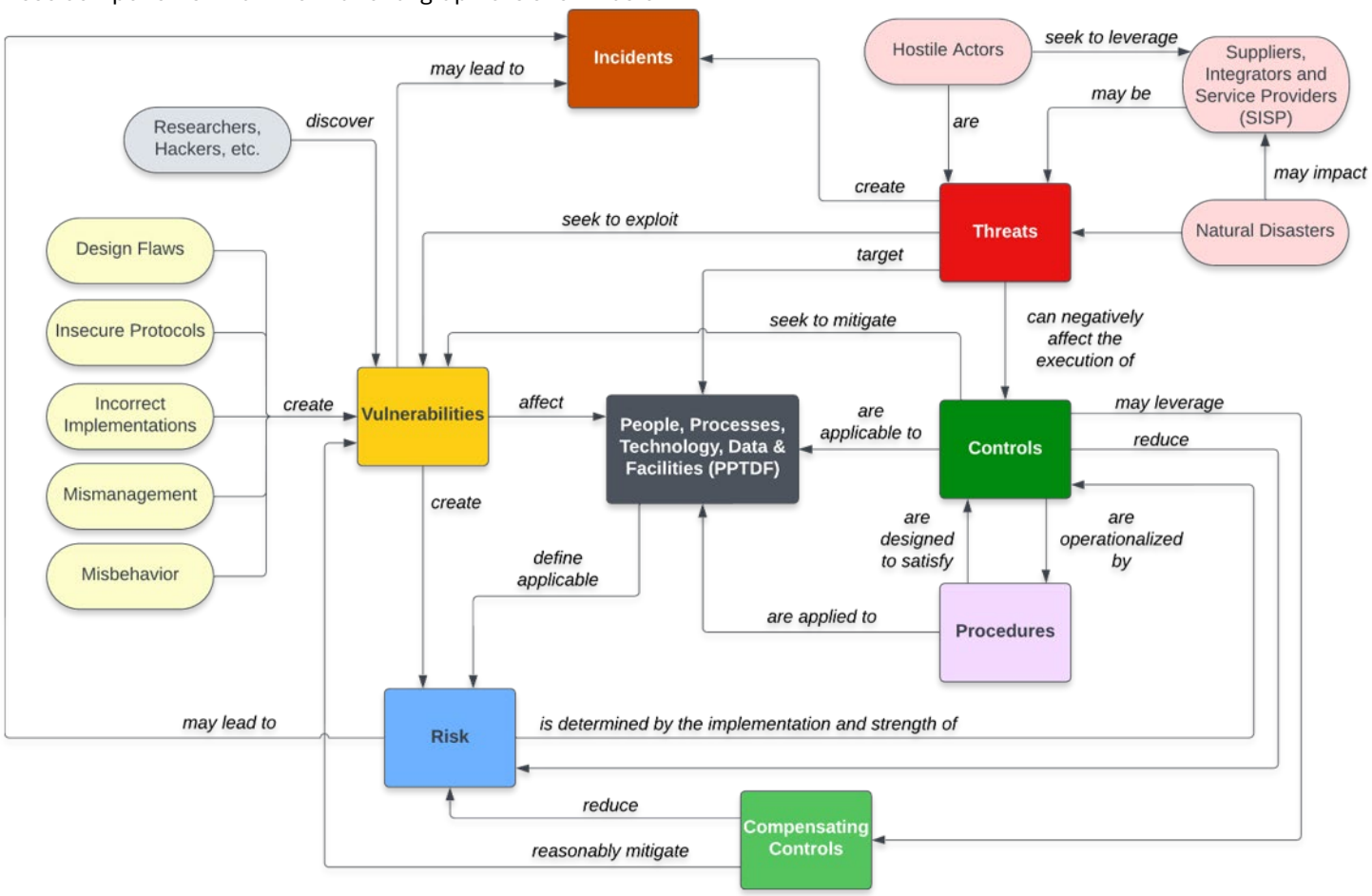
This guide is for educational purposes only. Users are encouraged to work with a competent professional to validate any compliance-related assumptions.

Understanding The Differences: Threats vs Vulnerabilities vs Risks

Risks and threats both tie into security, compliance and resilience 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:[31]



What Is A Risk?

In the context of security, compliance and resilience 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 security, compliance and resilience practices, "threat" is defined as:

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

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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.[32]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a desired result.[33]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.[34]

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 include:

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

---

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

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

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Risk Matrix		Occurrence Likelihood					
		Remote *[<1% chance of occurrence]*	Highly Unlikely *[1% to 10% chance of occurrence]*	Unlikely [10% to 25% chance of occurrence]	Possible [25% to 70% chance of occurrence]	Likely [70% to 99% chance of occurrence]	Almost Certain [>99% chance of occurrence]
Impact Effect	Catastrophic						
	Critical						
	Major						
	Moderate						
	Minor						
	Insignificant						

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 include, 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 security, compliance and resilience 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

- 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)

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 security, compliance and resilience 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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 security, compliance and resilience governance practices.
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a Severe 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 security, compliance and resilience governance practices.
- Do not have cyber-related liability insurance.

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

- Startups
- 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."* [35]

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

[35] *SCF Cybersecurity Materiality - https://securecontrolsframework.com/cybersecurity-materiality/*

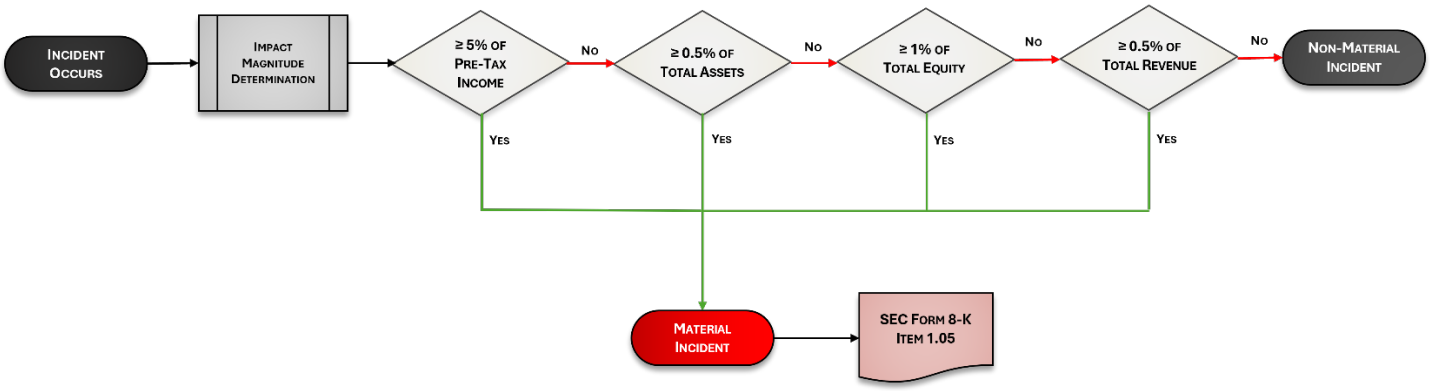
© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

meet one or more of the following criteria where the potential financial impact is:[36]

- ≥ 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: [37]



Historical Context For Security, Compliance and Resilience 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."* [38]
- 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."* [39]

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.

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.

[36] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*
[37] *SEC Cybersecurity Final Rule - https://www.sec.gov/files/rules/final/2023/33-11216.pdf*
[38] *SEC - https://www.sec.gov/comments/265-24/26524-77.pdf*
[39] *IFRS - https://www.ifrs.org/content/dam/ifrs/project/definition-of-materiality/definition-of-material-feedback-statement.pdf*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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:[40]

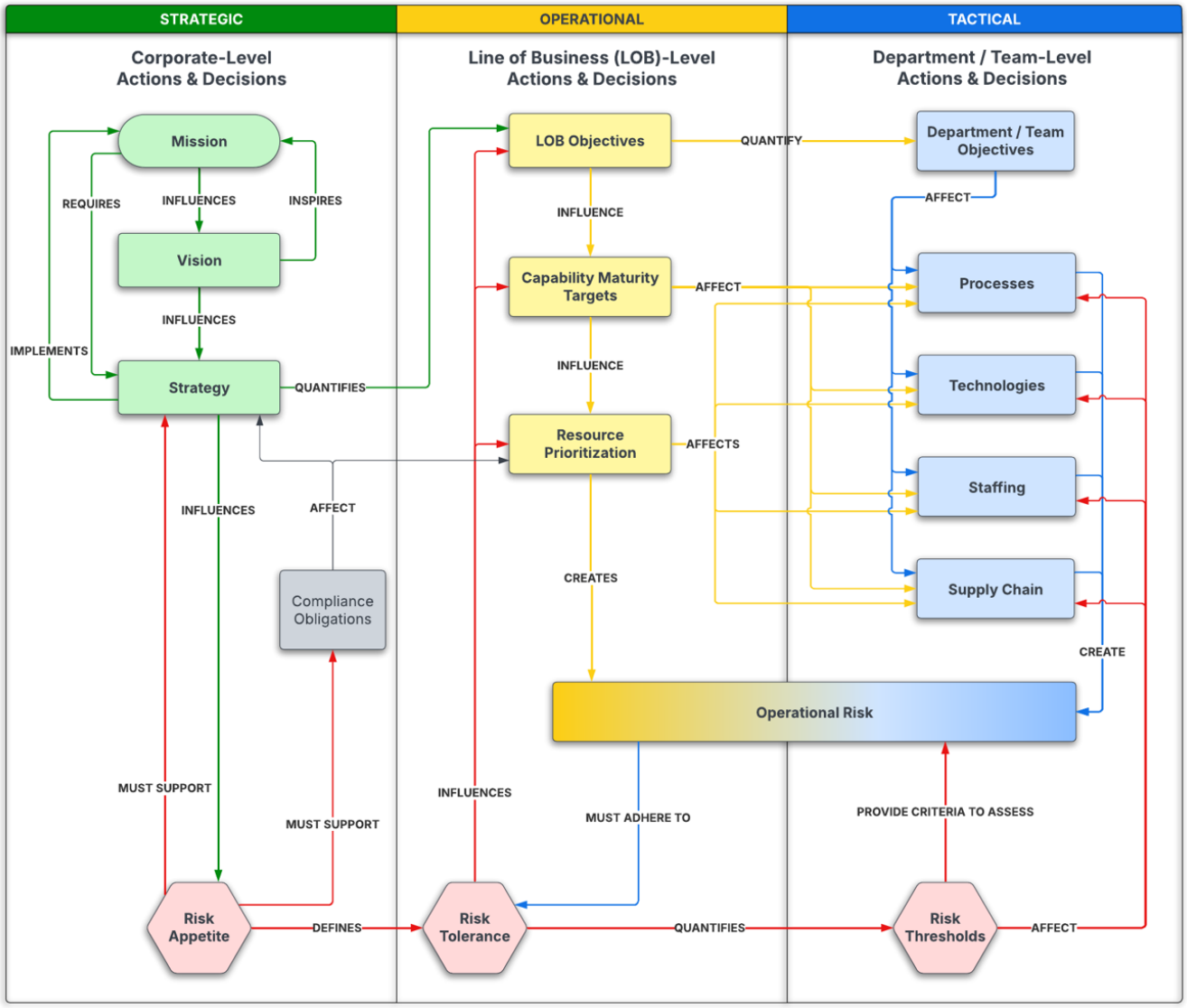
- At the strategic layer, where corporate-level actions and decisions are made, the organization's risk appetite is defined. The scope of the risk appetite can be organization-wide or compartmentalized to provide enhanced granularity.
- At the operational level, where Line of Business (LOB)-level actions 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.

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

This graphic can be downloaded:[41]



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.

[41] *ComplianceForge Risk Appetite vs Risk Tolerance vs Risk Thresholds* - https://content.complianceforge.com/pdf/risk-appetite-vs-risk-tolerance-vs-risk-thresholds.pdf

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

This guide is for educational purposes only. Users 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;

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

    - 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 9. 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 sixty-five (65) risks:

Risk Grouping	Risk #	Risk	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	Loss of Accountability / Attribution	Actions, transactions, asset ownership or other relevant activity cannot be reliably attributed to an accountable individual, service or system, impairing traceability, non-repudiation and enforcement.
	R-AC-2	Excessive or Unauthorized Privilege	Users, services or systems obtain or retain privileges beyond those required for authorized duties, increasing the ability to access, change, disclose or disrupt protected resources.
	R-AC-3	Unauthorized Privilege Elevation	An actor, account, service or process gains privileges beyond its authorized level, enabling access to restricted functions, data or administrative capabilities.
	R-AC-4	Unauthorized Access	Individuals, groups, services, devices or processes gain access to Technology Assets, Applications, Services, Data and/or Facilities (TAASDF) without appropriate authorization.
	R-AC-5	Identity Compromise / Impersonation	A user, service or machine identity is compromised, spoofed or hijacked, allowing an unauthorized actor to authenticate or operate as a trusted identity.
Asset Management	R-AM-1	Loss, Theft or Damage of Assets	Technology, data, equipment or other organizational assets are lost, stolen, destroyed, damaged or otherwise rendered unavailable for authorized use.
	R-AM-2	Unauthorized Modification / Loss of System Integrity	Unauthorized or unintended changes alter the configuration, code, data or state of a Technology Asset, Application and/or Service (TAAS) causing it to operate in an untrusted or unreliable manner.
	R-AM-3	Unauthorized Retention / Inability to Dispose of Data	Sensitive and/or regulated data is retained beyond authorized or necessary periods, cannot be reliably located or disposed of, or remains recoverable after intended destruction, creating security, data privacy, legal or discovery exposure.
Business Continuity	R-BC-1	Business / Service Interruption	Critical business processes, mission functions and Technology Assets, Applications and/or Services (TAAS) become unavailable, materially degraded or unable to meet required service levels.
	R-BC-2	Data Loss / Integrity Compromise	Data is destroyed, unavailable, corrupted, altered or otherwise loses required integrity or recoverability, impairing business, legal or operational use.
	R-BC-3	Reduced Operational Productivity	Personnel, systems and/or business processes operate below required efficiency or throughput because necessary

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

			Technology Assets, Applications, Services and/or Data (TAASD) are unavailable or degraded.
	R-BC-4	System / Data Compromise (Technical Vector)	Technology Assets, Applications and/or Services (TAAS) experience a technical attack vector compromise that results in unauthorized access, disclosure, modification, destruction or disruption (e.g., malware, phishing, hacking, etc.).
	R-BC-5	System / Data Compromise (Non-Technical Vector)	Technology Assets, Applications, Services and/or Data (TAASD) experience a non-technical attack vector compromise that results in unauthorized access, disclosure, modification, destruction or disruption (e.g., social engineering, sabotage, etc.).
Exposure	R-EX-1	Revenue Loss	The organization experiences reduced current or future revenue because a control deficiency disrupts operations: (1) Causes customer loss; (2) Prevents sales; and/or (3) Otherwise impairs revenue-generating activity.
	R-EX-2	Contractual Default / Termination	The organization breaches, defaults on, loses, terminates or fails to renew a contract because it cannot meet required security, data privacy, compliance, resilience and/or performance obligations.
	R-EX-3	Loss of Competitive Advantage	The organization loses market position, strategic differentiation, intellectual advantage or customer preference because a control deficiency (1) Exposes data; (2) Disrupts performance; and/or (3) Weakens stakeholder confidence.
	R-EX-4	Reputational Harm / Loss of Stakeholder Trust	Customers, partners, regulators, investors, employees or the public lose confidence in the organization, resulting in: (1) Reputational damage; and/or (2) Diminished brand value.
	R-EX-5	Regulatory / Legal / Contractual Financial Liability	The organization incurs fines, penalties, judgments, remediation, settlements, damages, indemnification costs or other financial liability due to legal, regulatory or contractual noncompliance.
	R-EX-6	Exposure from Unaddressed Vulnerabilities	Known Exploited Vulnerabilities (KEV) remain exploitable because they are not remediated, mitigated or otherwise addressed, increasing exposure to compromise.
	R-EX-7	System / Service Compromise	Technology Assets, Applications and/or Services (TAAS) are compromised, resulting in loss of confidentiality, integrity, availability, authenticity and/or safety.
	R-EX-8	Failure to Achieve Strategic / Mission Objectives	A control deficiency materially prevents, delays or degrades the organization's ability to achieve strategic, mission or program objectives.
	R-EX-9	Intellectual Property / Trade Secret Loss	The strategic or competitive value of proprietary data, trade secrets, research, designs, source code or other Intellectual Property (IP) is reduced when it is: (1) Improperly disclosed; (2) Stolen; (3) Copied; and/or (4) Rendered non-exclusive,

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

	R-EX-10	Fraud / Theft / Direct Financial Loss	The organization or its stakeholders suffer direct monetary loss through: (1) Fraud; (2) Theft; (3) Unauthorized transactions; (4) Diversion of funds; or (5) Other financially harmful activity.
	R-EX-11	Loss of Authorization / Certification / License	The organization loses or is unable to obtain or maintain an authorization, certification, accreditation, license or other permission required to operate, sell, contract or access a market.
Governance	R-GV-1	Failure to Support Business / Mission Objectives	Security, data privacy, compliance or resilience deficiencies prevent Technology Assets, Applications, Services and/or Data (TAASD) from reliably supporting required business operations, mission functions or strategic objectives.
	R-GV-2	Unaddressed Security / Compliance Exposure	Incorrect or incomplete control scoping leaves applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) without required safeguards, creating unmanaged security, data privacy, compliance and/or resilience exposure.
	R-GV-3	Unperformed / Unowned Control Responsibilities	Required security, data privacy, compliance and/or resilience activities are not performed, coordinated or escalated because responsibility or accountability is unclear or unassigned.
	R-GV-4	Uncontrolled Internal Security / Privacy Exposure	Internal practices are insufficient to prevent, detect, respond to or recover from security, data privacy, compliance and/or resilience events, leaving organizational operations and assets exposed.
	R-GV-5	Uncontrolled Third-Party Security / Privacy Exposure	Weak third-party governance or Cybersecurity Supply Chain Risk Management (C-SCRM) practices leave the organization exposed to security, data privacy, compliance, resilience or dependency risks originating from suppliers and External Service Providers (ESP).
	R-GV-6	Lack of oversight of internal controls	Internal control deficiencies, failures or changes remain unidentified or unresolved, allowing risk exposure to persist and reducing the organization's ability to demonstrate due diligence and due care.
	R-GV-7	Lack of oversight of third-party controls	Third-party control deficiencies, failures or changes remain unidentified or unresolved, allowing supplier-originated exposure to persist and reducing the organization's ability to demonstrate appropriate Third-Party Risk Management (TPRM) oversight.
	R-GV-8	Harm from Illegal, Abusive or Unsafe Content / Conduct	Illegal, abusive, threatening or otherwise harmful content or conduct causes: (1) Operational disruption; (2) Legal exposure; (3) Personnel harm; (4) Loss of trust; and/or (5) Other adverse organizational consequences.
	R-GV-9	Inability to Demonstrate Due Diligence / Due Care	The organization cannot produce defensible evidence that applicable risks, controls and obligations were reasonably identified, implemented, monitored and/or governed.
	R-GV-10	Unreliable Assurance / Decision Information	Executive management, the Board of Directors (BoD), assessors or other stakeholders rely on inaccurate, incomplete or untimely control, risk or compliance information, leading to: (1) Unsound decisions; and/or (2) False assurance.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Incident Response	R-IR-1	Loss of Investigative / Evidentiary Capability	Required evidence, logs, records or chain-of-custody integrity are unavailable or unreliable that prevents the organization from reliably: (1) Reconstructing; (2) Investigating; (3) Attributing / taking legal action for; and/or (4) Learning from an incident.
	R-IR-2	Delayed Containment / Increased Incident Impact	An incident is not contained, eradicated, communicated or escalated in a timely and appropriate manner, allowing the scope, duration, cost and/or harm of the incident to increase.
	R-IR-3	Incident Persistence / Recurrence	Root causes, persistence mechanisms or affected conditions are not effectively remediated, allowing the incident, vulnerability or compromise to continue or recur.
	R-IR-4	Incident Response / Recovery Cost	The organization incurs unplanned investigation, containment, recovery, notification, legal, forensic, restoration and/or other costs associated with managing an incident or loss event.
Operational Resilience	R-OR-1	Recovery Failure / Unacceptable Recovery Delay	The organization cannot restore critical services, data, facilities or capabilities within required recovery objectives after a disruption.
	R-OR-2	Concentration / Single-Point Dependency Failure	Failure of a highly concentrated supplier, technology, facility, region or other dependency causes disproportionate disruption because adequate alternatives or redundancy are unavailable.
Situational Awareness	R-SA-1	Undetected / Delayed Detection of Adverse Activity	Malicious, abnormal, unauthorized or otherwise material activity is not detected or recognized in time to prevent or limit harm.
	R-SA-2	Lack of a security-minded workforce	Personnel are more likely to: (1) Make unsafe decisions; (2) Fall victim to social engineering; (3) Mishandle data; (4) Violate requirements; and/or (5) Fail to recognize and report security or privacy concerns.
Supply Chain	R-SC-1	Third-Party Cybersecurity Compromise / Exposure	A supplier or External Service Provider (ESP) experiencing a cybersecurity weakness, incident or compromise causes loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) in organizational products, services, data or operations.
	R-SC-2	Third-Party Physical Security Disruption / Exposure	A physical security event affecting a supplier's or External Service Provider's (ESP) facilities, personnel, equipment or other assets disrupts or compromises products, services, data or operations relied upon by the organization.
	R-SC-3	Sub-Tier / Fourth-Party Supply Chain Exposure	Risks originating from a supplier's or External Service Provider's (ESP) own suppliers, subcontractors or dependencies propagate through the supply chain and affect organizational Confidentiality, Integrity, Availability and/or Safety (CIAS), compliance and/or operations.
	R-SC-4	Third-Party Legal / Compliance Exposure	Third-party noncompliance, unlawful conduct, sanctions, litigation or other legal conditions cause the organization to: (1) Violate obligations; (2) Lose contracts; (3) Incur legal and/or financial liability; and/or (4) Experience operational restrictions.
	R-SC-5	Harm from Unauthorized /	A product or service is used outside its authorized, intended or approved purpose, creating security, data privacy, safety, legal, operational or financial harm.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

		Unintended Product or Service Use	
	R-SC-6	Third-Party Dependency Failure	A critical third-party product, service or capability becomes unavailable, degraded, discontinued or otherwise unable to support required operations, causing business operations disruption.
	R-SC-7	Counterfeit / Non-Conforming Component Impact	Counterfeit, substituted, defective or non-conforming products or components cause reliability, security, safety, warranty or operational failures in organizational Technology Assets, Applications and/or Services (TAAS).
Artificial Intelligence & Autonomous Technologies	R-AI-1	AI Output / Decision Integrity Failure	An Artificial Intelligence (AI) model produces inaccurate, manipulated, biased, unsafe or otherwise unreliable outputs or decisions that cause dependent controls, users or processes to act incorrectly.
	R-AI-2	AI Data Confidentiality / Integrity / Provenance Loss	Training, fine-tuning, embedding, retrieval or inference data is disclosed, altered, contaminated, misattributed or stripped of required provenance, undermining data privacy, security or Artificial Intelligence (AI) reliability.
	R-AI-3	Unauthorized / Harmful Autonomous Action	An Artificial Intelligence (AI) agent or autonomous system takes an action outside authorized scope or intended objectives, causing security, data privacy, safety, legal, financial and/or operational harm.
	R-AI-4	Sensitive Data / Compliance Exposure from Unsanctioned AI Use	Unapproved or ungoverned Artificial Intelligence (AI) use: (1) Exposes sensitive and/or regulated data; (2) Creates unauthorized processing; (3) Introduces Intellectual Property (IP) or licensing issues; and/or (4) Causes statutory, regulatory and/or contractual noncompliance.
	R-AI-5	Unintended or Unsafe Technology Behavior	Artificial Intelligence (AI) exhibits emergent, unanticipated or unintended behavior that produces incorrect, unsafe or harmful outcomes or causes dependent controls and processes to operate outside intended boundaries.
	R-AI-6	AI Bias / Discriminatory Outcome	Artificial Intelligence (AI)-supported decisions or outputs produce unjustified, systematically biased or discriminatory outcomes that create legal, ethical, reputational or individual harm.
Operational Technology (OT)	R-OT-1	OT Safety / Process Availability Failure	Failure or compromise of Operational Technology (OT) or Industrial Control System (ICS) functions causes: (1) Loss or degradation of safety functions; (2) Physical-process availability; and/or (3) Equipment integrity / unsafe operating conditions.
Information Protection	R-IP-1	Long-Term Confidentiality Loss from Cryptographic Obsolescence	Sensitive and/or regulated data requiring long confidentiality lifetimes becomes susceptible to Harvest Now, Decrypt Later (HNDL) collection and future decryption.
	R-IP-2	Loss of Confidentiality	Sensitive and/or regulated data is disclosed or made accessible to unauthorized: (1) Individuals; (2) Entities; and/or (3) Technology Assets, Applications and/or Services (TAAS).
	R-IP-3	Loss of Data Integrity	Data is altered, corrupted, fabricated, deleted or otherwise changed without authorization or reliable detection, causing it to become untrustworthy for its intended use.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

	R-IP-4	Loss of Data / Service Availability	Technology Assets, Applications, Services and/or Data (TAASD) are unavailable or inaccessible when required to support authorized business or mission needs.
	R-IP-5	Loss of Authenticity / Provenance	The organization cannot reliably establish the origin, authenticity, lineage or trustworthiness of: (1) Data; (2) Software; (3) System components; (4) Communications; and/ or (5) Transactions.
	R-IP-6	Privacy Harm / Unauthorized Processing	Individuals are harmed and/or the organization is exposed to statutory and/or regulatory actions when Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed of without appropriate: (1) Authority; (2) Transparency; (3) Limitation; and/or (4) Protection,
Safety	R-SF-1	Injury / Loss of Life	A control deficiency contributes to unsafe conditions that cause or materially increase the likelihood of: (1) Human injury; (2) Illness; and/or (3) Loss of life.
	R-SF-2	Physical / Environmental Damage	A control deficiency contributes to damage or destruction of: (1) Physical assets; (2) Facilities; (3) Equipment; and/or (4) The environment.
Personnel	R-PE-1	Loss of Critical Knowledge / Capability	The organization loses essential knowledge, skills, authority or operational capability because critical personnel are unavailable, depart or cannot perform required duties.

SCF Threat Catalog

It is necessary to develop a threat catalog that identifies possible natural and man-made threats that affect the entity's security, compliance and resilience 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	Insufficient precipitation or water availability that restricts municipal, industrial or facility water supplies and can impair cooling, fire suppression, sanitation, facility operations or dependent utility services.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

NT-2	Earthquakes	Sudden ground movement caused by seismic activity that can damage facilities, technology, utilities and transportation infrastructure, disrupt personnel access and impair the operation or recovery of controls.
NT-3	Fire & Wildfires	Fire affecting a facility or surrounding area that can injure personnel, destroy or damage technology and records, interrupt utilities and facility access and impair primary or recovery control capabilities.
NT-4	Floods	Water intrusion or inundation caused by rainfall, surface water, storm surge, infrastructure failure or other sources that can damage facilities and technology, interrupt utilities and make control-supporting locations inaccessible.
NT-5	Hurricanes & Tropical Storms	A hurricane, tropical storm or other tropical cyclone that can produce destructive winds, flooding, storm surge, utility outages, transportation disruption and facility damage that impair control execution or recovery.
NT-6	Landslides & Debris Flow	Movement of soil, rock or debris that can damage or isolate facilities, transportation routes, utilities and communications needed to execute or recover controls.
NT-7	Pandemic (Disease) Outbreaks	A widespread infectious disease event that can reduce workforce availability, disrupt suppliers and essential services, restrict facility access and degrade the organization's ability to operate, monitor or recover controls.
NT-8	Severe Weather	Severe meteorological conditions, including high winds, hail, extreme heat, heavy precipitation or similar events, that can damage facilities or technology, disrupt utilities and transportation, or otherwise degrade control execution.
NT-9	Space Weather	Solar or geomagnetic activity that can disrupt satellites, radio communications, navigation, timing services, electrical grids or other technologies on which control execution depends.
NT-10	Thunderstorms & Lightning	Thunderstorms or lightning that can cause electrical surges, fires, utility outages, communications disruption or equipment damage that impairs control execution.
NT-11	Tornadoes	A tornado or associated severe wind event that can damage facilities, equipment, utilities and transportation infrastructure, endanger personnel and interrupt the operation or recovery of controls.
NT-12	Tsunamis	A tsunami or related coastal inundation event that can cause rapid flooding, structural damage, utility disruption, loss of access and widespread damage to control-supporting facilities and infrastructure.
NT-13	Volcanoes	Volcanic activity, including eruption, ashfall, lava, gases or related seismic effects, that can damage or contaminate facilities and equipment, disrupt transportation and utilities and impair control execution.
NT-14	Winter Storms & Extreme Cold	Snow, ice, freezing temperatures or other severe winter conditions that can interrupt utilities and transportation, damage equipment, restrict personnel access and degrade control execution or recovery.

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 thirty-one (31) manmade threats:

Threat #	Threat	Threat Description
MT-1	Civil or Political Unrest	Civil disturbance, protest activity, political instability or related violence that can restrict personnel or facility access, disrupt transportation and utilities, damage assets, interrupt suppliers or otherwise impair control execution.
MT-2	Malicious Cyber Activity	Deliberate malicious cyber activity, including exploitation, malware, credential abuse, denial-of-service, social engineering or other attack techniques, that can disable, bypass, manipulate or otherwise impair controls and their supporting technologies.
MT-3	Hazardous Materials Emergencies	An accidental release, spill, leak, fire, explosion or other hazardous-materials event that can endanger personnel, require evacuation, damage facilities or interrupt operations and control-supporting infrastructure.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

MT-4	Nuclear, Biological and Chemical (NBC) Weapons	Intentional use or release of chemical, biological, radiological or nuclear agents that can cause casualties, contamination, evacuation, infrastructure disruption and prolonged loss of access to facilities or resources needed for control execution.
MT-5	Physical Crime	Physical criminal activity that results in unauthorized entry, theft, vandalism, sabotage or damage to facilities, equipment, records or other assets needed for control execution.
MT-6	Terrorism & Armed Attacks	Terrorist activity, active-assailant events or other armed attacks that can cause casualties, facility damage, evacuation, loss of access, infrastructure disruption or interruption of control-supporting operations.
MT-7	Utility Service Disruption	Sustained or material loss or degradation of electricity, water, natural gas, telecommunications, internet connectivity or other utility services required to operate facilities, technologies or controls.
MT-8	Dysfunctional Management Practices	Management interference, direction, override or other intentional circumventions that prevents established controls from being performed, enforced, monitored or escalated as designed.
MT-9	Human Error	Unintentional action or omission by personnel, contractors or other authorized users that misconfigures, disables, bypasses, damages or otherwise impairs a control or its supporting technology, process or data.
MT-10	Technical / Mechanical Failure	Non-malicious failure, degradation or malfunction of hardware, software, communications, mechanical equipment or supporting infrastructure that causes a control to become unavailable, unreliable or ineffective.
MT-11	Statutory / Regulatory / Contractual Change	A change in applicable laws, regulations, government directives or contractual obligations that invalidates existing assumptions, requires different safeguards, restricts technologies or suppliers, or otherwise causes established controls to become insufficient or inoperable.
MT-12	Data Quality Degradation / Data Poisoning	Use or introduction of inaccurate, stale, corrupted, incomplete, manipulated or otherwise untrustworthy data that causes controls, analytics or automated decisions to operate incorrectly or ineffectively.
MT-13	Artificial Intelligence & Autonomous Technologies (AAT) System Failure or Unintended Behavior	Non-malicious failure, malfunction, hallucination, unsafe output, goal misalignment, unintended autonomous action or other erroneous behavior by Artificial Intelligence & Autonomous Technologies that impairs a control or dependent business process.
MT-14	Fraud, Corruption and/or Intentional Criminal Conduct	Intentional criminal or corrupt conduct by an insider, third party or other actor that can bypass, manipulate or disable controls (e.g., fraud, bribery, theft, embezzlement, extortion or deliberate policy circumvention).
MT-15	Conflict of Interest (COI) / Undue Influence / Insider Misconduct	A Conflict of Interest (COI) or improper influence that causes a person with authority or access to make biased decisions, circumvent safeguards, conceal issues or otherwise impair objective control execution.
MT-16	Economic Shock / Market Disruption	Material economic instability, recession, inflation, interest-rate or exchange-rate shocks, commodity volatility or similar macroeconomic conditions that disrupt staffing, suppliers, investment or resources needed to sustain control execution.
MT-17	Foreign Ownership, Control, or Influence (FOCI)	Foreign Ownership, Control or Influence (FOCI) that is used to shape decisions, compel access, redirect operations or obtain sensitive information in a manner that can bypass or undermine organizational or supply-chain controls.
MT-18	Geopolitical Conflict / Government Intervention	Political conflict, government intervention, war, civil instability, nationalization, export restriction or other geopolitical action that disrupts suppliers, infrastructure, communications, access or resources required for control execution.
MT-19	Sanctions / Trade Restriction Disruption	Imposition, expansion or enforcement of sanctions, export controls, exclusions or trade restrictions that removes or constrains access to suppliers, technologies, services, personnel or financial channels required for control execution.
MT-20	Counterfeit / Non-Conforming Products	Counterfeit, substituted, defective or non-conforming components, materials, software or services enter the supply chain and cause control-supporting products to perform unpredictably, fail prematurely or operate outside required specifications.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

MT-21	Hazardous / Degraded Operational Environment	Environmental, physical or operating conditions at the place of performance that exceed design assumptions or safe operating limits and degrade personnel, equipment or processes needed for control execution.
MT-22	Manufacturing Capacity / Supply Disruption	Loss, reduction or delay of manufacturing capacity, materials, components or supplier output that prevents timely availability of products or services required for control execution (e.g., sole-source or concentration failures).
MT-23	Product Defect / Design Failure	A design flaw, manufacturing defect, quality failure or specification deviation in a product or service that causes unsafe, unreliable or ineffective operation of a control or its supporting technology.
MT-24	Supplier Financial Distress / Insolvency	Financial distress, loss of liquidity, hostile acquisition, bankruptcy or insolvency of a critical supplier that interrupts contractual performance, support, maintenance or delivery of control-dependent products or services.
MT-25	Workforce Shortage / Loss of Critical Skills / Labor Disruption	Loss, shortage, unavailability or labor disruption of personnel with required knowledge, skills or authorization that prevents controls from being performed, maintained, monitored or recovered as intended.
MT-26	Transportation / Logistics Disruption	Accident, cargo loss, carrier failure, route closure, capacity shortage or other transportation or logistics disruption that delays or prevents delivery of products, equipment or services needed for control execution.
MT-27	Infrastructure Failure / Degradation	Failure, degradation or unavailability of transportation, communications, energy, facilities or other foundational infrastructure on which the organization or its supply chain depends for control execution.
MT-28	Harvest Now / Decrypt Later (HNDL)	A threat actor intercepts and retains currently encrypted sensitive information with the intent to decrypt it later when cryptanalytic or quantum capabilities make the deployed cryptography vulnerable.
MT-29	Adversarial Artificial Intelligence (AI) Attack	Deliberate manipulation or exploitation of an AI system through adversarial inputs, prompt injection, jailbreaking, data or model poisoning, model theft, inference attacks or related techniques that bypass, alter or impair controls or AI-dependent functions.
MT-30	Operational Technology (OT) / Industrial Control System (ICS) Attack	Deliberate cyberattack against Operational Technology (OT) or Industrial Control System (ICS) environments that manipulates, disrupts or disables industrial processes, safety functions, equipment or control-supporting operations.
MT-31	Cryptographic Compromise / Cryptanalytic Capability Advancement	Advances in computing, cryptanalysis or attack techniques reduce the effective security of deployed cryptographic algorithms or key sizes, causing cryptographic controls to provide less protection than intended.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 10. EVIDENCE REQUEST LIST (ERL)

The SCF contains an Evidence Request List (ERL) tab to support the SCR Conformity Assessment Program (SCR 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	F
1	#	SCF 2026.3 ERL #	Area of Focus	ERL Artifact	Evidence Request List (ERL) Artifact Description	SCF Control Mappings
17	16	E-AST-02	Asset Management	Asset Scoping Guidance	Documented evidence of an asset scoping guidance. This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on defining in-scope Technology Assets, Applications, Services and/or Data (TAASD) (including third-parties).	AST-16 AST-16.1 AST-17.1 CPL-03 IAO-03
18	17	E-AST-03	Asset Management	Asset Disposal Evidence	Documented evidence of asset disposal/destruction (e.g., asset tracking by serial # for shredding, degaussing, etc.).	AST-22 AST-36 DCH-17 DCH-18 DCH-18.2
19	18	E-AST-04	Asset Management	Asset Inventories - Hardware	Documented evidence of an inventory of the organization's technology hardware assets.	AST-03 AST-04
20	19	E-AST-05	Asset Management	Asset Inventories - Software	Documented evidence of an inventory of the organization's software assets.	AST-04
21	20	E-AST-06	Asset Management	Asset Inventories - Cloud Service Provider (CSP)	Documented evidence of an inventory of the organization's cloud-based services (e.g., SaaS, IaaS, PaaS, etc.).	CLD-02 TPM-08
22	21	E-AST-07	Asset Management	Cyber-Physical Systems (CPS)	Documented evidence of an inventory of the organization's physical assets that process functions based on software and networks.	AST-04 EMB-04
23	22	E-AST-08	Asset Management	Asset Inventories - Sensitive / Regulated Data	Documented evidence of an inventory of the organization's sensitive/regulated data (including systems where sensitive/regulated data is stored, processed and/or transmitted) that contains sufficient information to determine the potential impact in the event of a data loss incident.	CLD-10 DCH-05 DCH-10 PRI-07

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Section 11. Assessment Objectives (AOs)

The SCF contains an Assessment Objectives (AOs) tab to support the SCR Conformity Assessment Program (SCR 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	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)	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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 12. 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.[42] 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.

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 13. 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 starting points for organizations needing a push in the right direction for possible controls to address pre-defined topics.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Section 14. 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 security, compliance and resilience 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 1,500 cybersecurity & data protection controls is categorized into thirty-four (34) domains that are mapped to over 200 authoritative sources (e.g., statutory, regulatory and contractual frameworks). Those applicable SCF controls can operationalize the security, compliance and resilience principles to help an organization ensure that secure practices are implemented by design and by default.

You may be asking yourself, *"What security, compliance and resilience principles should I be using?"* and that is a great question. The SCF helped with this common question by taking the thirty-four (34) 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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

secure systems, applications and processes that will by default help the organization comply with its compliance obligations.



Secure, Compliant & Resilient (SCR) Principles

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

The SCR is a set of thirty-four (34) security, compliance and resilience principles that leverage the SCF's extensive security, compliance and resilience control set. You can download the free poster from the SCF website.[43]

Steps To Operationalize The SCR Principles

1. Read through the SCR principles to familiarize yourself with the thirty-four (34) 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.

SCF Domains & SCR Principles

The SCR establishes thirty-four (34) common-sense principles to guide the development and oversight of a modern security, compliance and resilience program. Those thirty-four (34) SCR principles are listed below:

#	SCF Domain	SCF Identifier	Secure, Compliant & Resilient (SCR) Principles	Principle Intent
1	Secure, Compliant & Resilient Governance	GOV	Govern the organization's Secure, Compliant & Resilient Program (SCRP) through accountable oversight, evidence-based decision-making and defensible evidence that the organization is secure, compliant and resilient.	Organizations establish and maintain governance structures, decision rights, accountability mechanisms and documented evidence to demonstrate that security, compliance and resilience practices are designed, implemented, monitored and improved in a manner that can withstand scrutiny from leadership, regulators, auditors, customers and other interested parties.
2	Artificial Intelligence & Autonomous Technologies	AAT	Govern Artificial Intelligence & Autonomous Technologies (AAT) through trustworthy, secure and resilient lifecycle practices that manage intended and unintended outcomes.	Organizations ensure AAT capabilities are designed, developed, deployed, monitored and governed to be reliable, safe, fair, secure, resilient, transparent, explainable and privacy-enhancing, with risk management practices that address model, agent and autonomous decision-making risks.
3	Asset Management	AST	Manage Technology Assets, Applications and Services (TAAS) throughout their lifecycle to maintain visibility, accountability, authorization and protection.	Organizations maintain accurate inventories, ownership records and data relationships for TAAS from procurement through disposal to ensure only authorized assets, applications and services are used and associated data is protected throughout its lifecycle.

[43] *SCF Domains - https://content.securecontrolsframework.com/pdf/scf-security-compliance-resilience-scr-principles.pdf*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

4	Business Continuity & Disaster Recovery	BCD	Maintain resilient capabilities to sustain business-critical functions and recover from disruptions through documented, tested and maintained continuity and recovery processes.	Organizations establish, exercise and improve Business Continuity and Disaster Recovery (BC/DR) capabilities to minimize operational disruption from adverse events, meet recovery objectives and support business, legal, regulatory and stakeholder obligations.
5	Capacity & Performance Planning	CAP	Govern current and future capacity and performance requirements for Technology Assets, Applications, Services and Data (TAASD) to sustain reliable operations.	Organizations prevent avoidable business interruptions caused by capacity and performance limitations through baselines, thresholds, forecasting, demand planning and leadership visibility into current and future performance needs.
6	Change Management	CHG	Manage changes to Technology Assets, Applications, Services and Data (TAASD) through an authorized, risk-based process that evaluates, implements and validates changes before and after deployment.	Organizations ensure technology and business stakeholders assess, authorize, test, implement, monitor and validate changes to minimize production impact, preserve availability, support rollback and maintain secure configurations.
7	Cloud Security	CLD	Govern cloud services and environments through risk-based, cloud-native security, compliance and resilience practices aligned with shared responsibility obligations.	Organizations govern private, public and hybrid cloud environments, including IaaS, PaaS and SaaS, to manage shared responsibility risks, third-party dependencies, architectural decisions, data protection, portability and resilience requirements.
8	Compliance	CPL	Govern security, compliance and data protection obligations to maintain defensible evidence of conformity with applicable internal and external requirements.	Organizations identify, interpret, implement and maintain evidence of conformity with applicable statutory, regulatory, contractual and internal obligations to demonstrate due diligence and due care.
9	Configuration Management	CFG	Establish and enforce secure configuration baselines that implement least privilege and least functionality for Technology Assets, Applications and Services (TAAS) to support a defensible secure configuration posture.	Organizations establish, maintain, monitor and enforce secure configurations aligned with vendor recommendations and industry-recognized secure practices to preserve system integrity and prevent unauthorized or unintended functionality.
10	Continuous Monitoring	MON	Maintain situational awareness through centralized collection, correlation and analysis of security-relevant telemetry from Technology Assets, Applications and Services (TAAS).	Organizations establish enterprise-wide situational awareness through centralized collection, correlation, analysis and review of security-relevant events, telemetry and control status to reduce blind spots that could contribute to compromise, data exfiltration or TAAS unavailability.
11	Cryptographic Protections	CRY	Use appropriate cryptographic mechanisms and industry-recognized key management practices to protect sensitive and regulated data at rest and in transit.	Organizations protect the confidentiality and integrity of data through approved cryptographic technologies, key lifecycle management, cryptographic inventory practices and migration planning that

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

				supports secure, resilient and compliant cryptographic protections.
12	Data Classification & Handling	DCH	Enforce a standardized classification methodology to determine data sensitivity and support Technology Assets, Applications and Services (TAAS) criticality decisions, enabling appropriate data handling, protection, retention and disposal requirements.	Organizations classify Technology Assets, Applications, Services and Data (TAASD) and implement risk-appropriate handling, protection, retention and disposal safeguards to prevent unauthorized disclosure, modification or misuse of data throughout its lifecycle.
13	Embedded Technology	EMB	Apply risk-based security, compliance and resilience practices to embedded technologies where compromise or misuse could create operational, safety and/or data protection impacts.	Organizations develop, deploy, harden, monitor and maintain embedded technologies, including IoT and Operational Technology (OT), with safeguards for hardware, firmware, software, communications, service protocols and safety-related dependencies.
14	Endpoint Security	END	Harden and centrally manage endpoint devices to protect Technology Assets, Applications, Services and Data (TAASD) from unauthorized access, compromise and disruption.	Organizations protect endpoint devices and associated data through secure configuration, access control, malware protection, monitoring, response and lifecycle management practices aligned with applicable security, compliance and resilience obligations.
15	Human Resources Security	HRS	Execute security-informed personnel management practices that address screening, onboarding, acceptable behavior, role-based risk, competence and offboarding requirements.	Organizations cultivate a security, compliance and resilience-minded workforce by defining personnel security expectations, validating role-based competence, supporting appropriate culture and collaboration, and managing personnel risk throughout the employment lifecycle.
16	Identification & Authentication	IAC	Implement secure, compliant and resilient Identity and Access Management (IAM) capabilities that enforce least privilege across human users, devices, service accounts and other Non-Person Entities (NPEs).	Organizations enforce least privilege by limiting access to Technology Assets, Applications, Services and Data (TAASD) to authorized users, services and entities with Need to Know (NTK) / Need to Access (NTA) based on approved identities, authentication strength, attributes and access rights.
17	Incident Response	IRO	Maintain a tested incident response capability that enables trained responders to identify, analyze, contain, eradicate and recover from incidents according to documented Incident Response Plans (IRPs).	Organizations establish, maintain and exercise the capability to lawfully and effectively respond to cybersecurity incidents in a timely manner, preserve evidence and notify affected stakeholders as required.
18	Information Assurance	IAO	Execute Information Assurance (IA) practices to validate that expected security, compliance and resilience controls are appropriately designed and operating as intended for Technology Assets, Applications and Services (TAAS).	Organizations validate the adequacy and operating effectiveness of security, compliance and resilience controls across development, testing and production environments through assurance activities that support

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

				defensible risk and compliance decisions.
19	Maintenance	MNT	Proactively maintain Technology Assets, Applications and Services (TAAS) through authorized maintenance practices that preserve performance, security, compliance, resilience and supportability.	Organizations perform, monitor and document maintenance for TAAS, including third-party-supported or hosted technologies, to preserve operational effectiveness and apply additional scrutiny to end-of-life or unsupported components.
20	Mobile Device Management	MDM	Govern mobile device access to Technology Assets, Applications, Services and Data (TAASD) to reduce attack surface and data exposure.	Organizations manage risks associated with organization-owned, employee-owned and third-party-owned mobile devices through centralized, risk-based controls for device access, configuration, data storage, monitoring and remote management commensurate with ownership model and risk.
21	Network Security	NET	Architect and implement defense-in-depth network protections that segment, restrict and monitor access to Technology Assets, Applications, Services and Data (TAASD).	Organizations architect and operate security, compliance and resilience controls that protect the Confidentiality, Integrity, Availability and Safety (CIAS) of network infrastructure through segmentation, traffic control, secure connectivity and situational awareness of network activity.
22	Physical & Environmental Security	PES	Protect physical environments through layered physical security and environmental controls that safeguard physical and digital assets from unauthorized access, theft, damage and disruption.	Organizations limit physical access to Technology Assets, Applications, Services and Data (TAASD) and monitor environmental conditions commensurate with risk to prevent unauthorized access and reduce equipment failure, damage or disruption from physical and environmental threats.
23	Data Privacy	PRI	Execute risk-based and legally defensible data privacy practices that conform with applicable statutory, regulatory and contractual obligations to protect sensitive Personal Data (sPD) throughout its lifecycle.	Organizations govern and implement privacy practices that align with overall privacy strategy; meet statutory regulatory and contractual obligations; ensure privacy by design and by default; protect individual rights; and provide lawful processing and safeguards for sensitive Personal Data (sPD).
24	Project & Resource Management	PRM	Operationalize security, compliance and resilience objectives by integrating cybersecurity and data privacy requirements into project, program and resource management practices.	Organizations ensure security-related initiatives have defined ownership, funding, staffing, dependencies, schedules and project/program management support necessary for successful execution.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

25	Quantum Security	QTS	Mitigate quantum-enabled cryptographic risks through governance structures that operationalize Post-Quantum Cryptography (PQC) risk management practices.	Organizations identify, assess and mitigate risks associated with Cryptographically Relevant Quantum Computers (CRQCs), including risks that may render legacy cryptographic mechanisms ineffective, through cryptographic inventory, prioritization, migration planning and cryptographic agility.
26	Risk Management	RSK	Proactively identify, assess, prioritize and treat risks to align Technology Assets, Applications, Services and Data (TAASD)-related decisions with the organization's defined risk appetite and risk tolerance.	Organizations ensure business units and process owners understand their roles and responsibilities applicable to effective management of security, compliance, privacy and resilience risks, while cybersecurity and data privacy teams advise on risk matters and business stakeholders retain risk ownership.
27	Secure Engineering & Architecture	SEA	Apply industry-recognized secure engineering and architecture principles to deliver secure, compliant and resilient systems, applications and services.	Organizations align cybersecurity engineering and architecture decisions with the organization's technology strategy and industry-recognized practices, including secure-by-design, threat modeling, resilience engineering and defensible architecture decisions.
28	Security Operations	OPS	Deliver secure, compliant and resilient operations through defined processes, skilled personnel, monitoring, escalation and continuous improvement that effectively detect, isolate, and remediate cyber threats while ensuring business resilience.	Organizations establish resources, procedures, runbooks and management structures to deliver effective cybersecurity, physical security and data privacy operations aligned with organizational risk, service and resilience needs.
29	Security Awareness & Training	SAT	Foster a security, compliance and resilience-minded workforce through ongoing, role-based education on evolving threats, obligations and secure workplace practices.	Organizations develop and sustain a security, compliance and resilience-minded workforce through continuous education, awareness activities, practical exercises and role-based training that reinforces expected behaviors.
30	Technology Development & Acquisition	TDA	Develop and acquire Technology Assets, Applications and Services (TAAS) through secure-by-design, risk-informed and resilient lifecycle practices.	Organizations integrate security, compliance and resilience requirements into internally developed and acquired TAAS, including secure development practices, acquisition due diligence, supplier requirements, validation, acceptance criteria and least privilege/least functionality expectations.
31	Third-Party Management	TPM	Execute Supply Chain Risk Management (SCRM) practices to assess, select, contract, monitor and manage trustworthy third parties for product and service delivery.	Organizations minimize security, compliance and resilience risks associated with third parties through due diligence, contractual safeguards, ongoing monitoring, performance management, contingency planning and exit strategies.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

32	Threat Management	THR	Proactively identify, assess and manage threats to Technology Assets, Applications, Services and Data (TAASD) and business processes to inform risk decisions and corrective actions.	Organizations establish threat intelligence-informed capabilities to identify, assess, prioritize and manage technology-related and business-process threats to TAASD and determine appropriate risk responses.
33	Vulnerability & Patch Management	VPM	Reduce exploitable weaknesses in Technology Assets, Applications and Services (TAAS) through coordinated vulnerability identification, prioritization, remediation and validation practices.	Organizations manage technical vulnerabilities through asset-aware discovery, vulnerability assessment, risk-based prioritization, patch management, threat intelligence, remediation validation and change management practices.
34	Web Security	WEB	Protect Internet-facing Technology Assets, Applications and Services (TAAS) by minimizing attack surfaces and monitoring for anomalous activity.	Organizations reduce risks associated with Internet-accessible TAAS through secure configuration, web and Application Programming Interface (API) security controls, content and file integrity monitoring, logging, auditing and detection of malicious activity.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

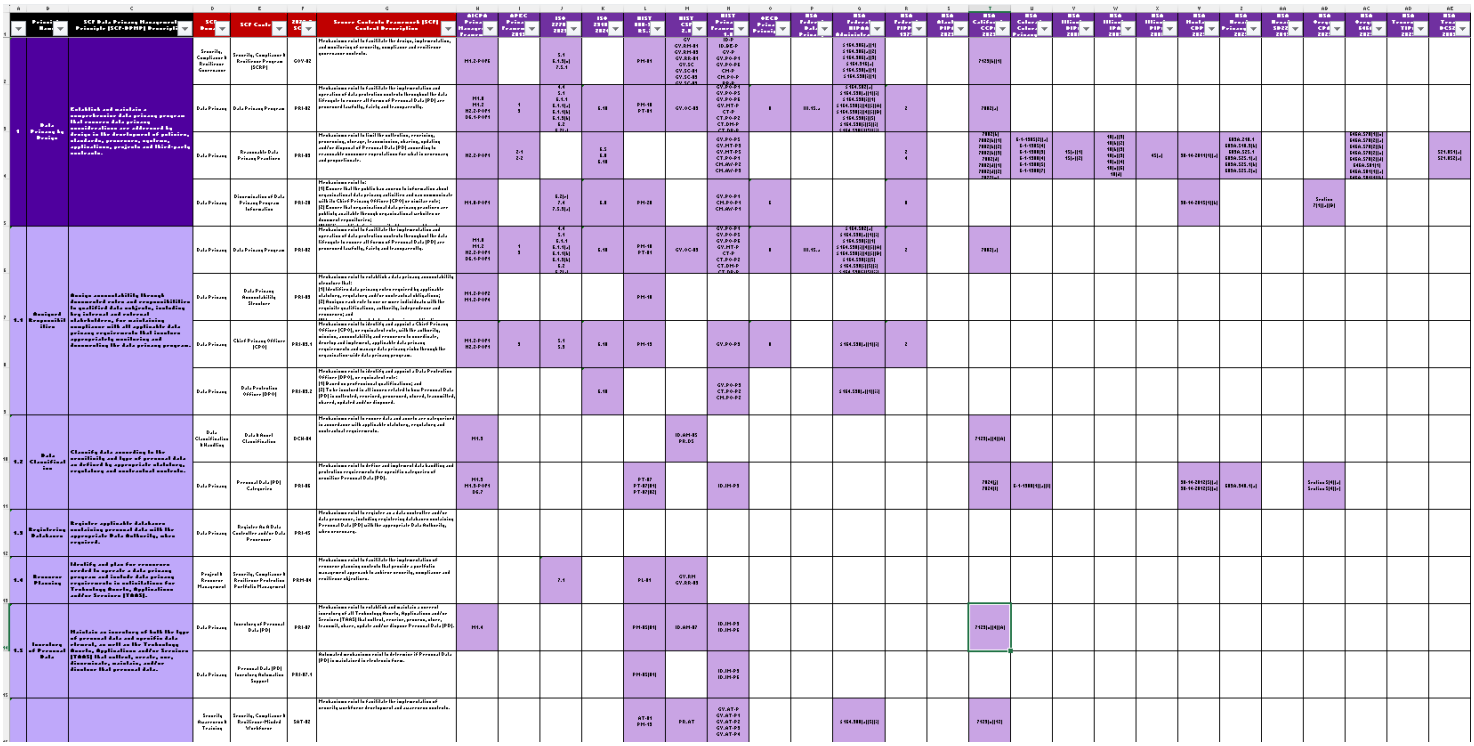
This guide is for educational purposes only. Users are encouraged to work with a competent professional to validate any compliance-related assumptions.

SECTION 15. 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 security, compliance and resilience 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 security, compliance and resilience considerations by default and by design. The DPMP is included in the SCF download as a separate tab in the Excel spreadsheet.[44]

Think of the SCF Data 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 security, compliance and resilience 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 over a dozen of the leading privacy frameworks and create a set of simplified, yet comprehensive, privacy management principles.

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-seven (87) principles of the SCF Data Privacy Management Principles are organized into eleven (11) domains:

1. Privacy by Design;

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

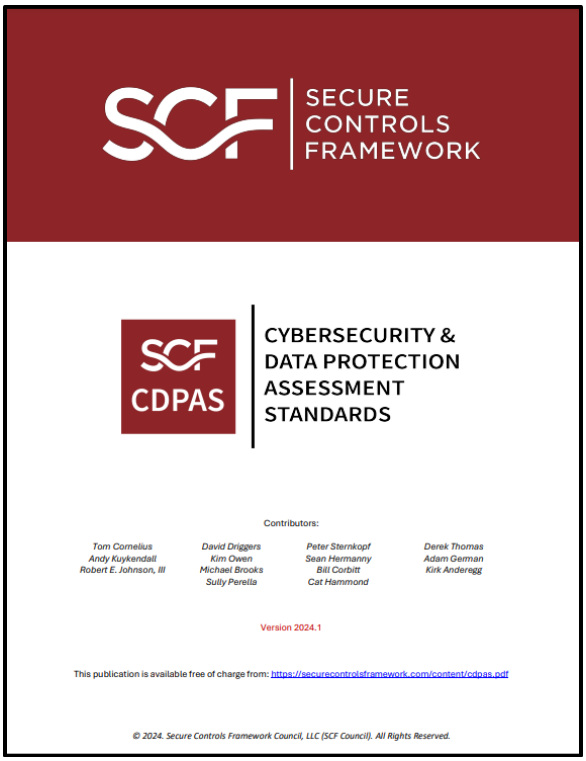
2. Data Subject Participation;
3. Limited Collection & Use;
4. Transparency;
5. Data Lifecycle Management;
6. Data Subject Rights;
7. Security by Design;
8. Incident Response;
9. Risk Management;
10. Third-Party Management; and
11. Business Environment.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 16. SCF CYBERSECURITY & DATA PROTECTION ASSESSMENT STANDARDS (CDPAS)

The Cybersecurity & Data Protection Assessment Standards (CDPAS) is a cohesive, consistent set of standards for performing security, compliance & resilience-related Third Party Assessment, Attestation and Certification Services (3PAAC Services). By following the Cybersecurity & Data Protection Assessment Standards (CDPAS) approach, security, compliance & resilience 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. [45]



CDPAS PURPOSE

The CDPAS exists to provide performance standards for security, compliance & resilience-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 security, compliance & resilience assessment strategies tailored to their specific mission, business needs, threats and operational environments.

CDPAS STANDARDS

The CDPASS can be downloaded from the SCF website. [46]

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

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SECTION 17. SCF MERGERS, ACQUISITIONS & DIVESTITURES (MA&D) SECURITY STANDARD (MADSS)

The SCF took on an ambitious project to "build a better mousetrap" to fix the common complaints associated with Mergers, Acquisitions & Divestitures (MA&D) due diligence. The Mergers, Acquisitions & Divestitures Security Standards (MADSS) is a standard to normalize MA&D-related assessment practices. [47]



MADSS PURPOSE

The MADDS exists to provide reasonable guidance for MA&D due diligence activities.

MADSS INTENT

The MADSS 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 organization. It can be modified, or augmented, with specific requirements. By following this methodology, cybersecurity and data privacy practitioners can improve the currently disjointed approach used to perform assessments of cybersecurity and/or data privacy controls.

MADSS STANDARDS

The MADSS can be downloaded from the SCF website. [48]

[47] *MADSS – https://securecontrolsframework.com/free-scf-content/mergers-acquisitions-divestitures-ma-d/*

[48] *MADSS download – https://securecontrolsframework.com/content/madss.pdf*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

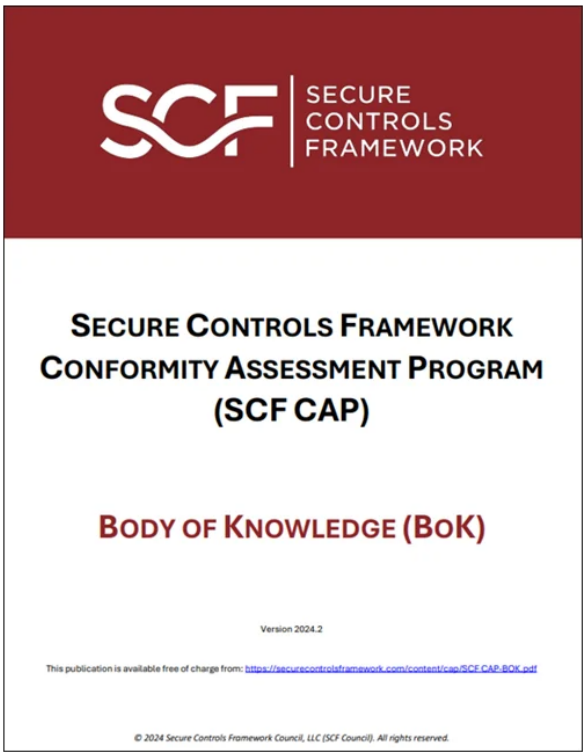
Section 18. Secure Controls Framework Conformity Assessment Program (SCR CAP)

The SCR Conformity Assessment Program (SCR CAP) is an organization-level conformity assessment.[49] The SCR CAP is designed to utilize tailored security, compliance and resilience 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 security, compliance and resilience-specific laws, regulations and frameworks.

The SCR 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 SCR CAP is unique in its metaframework approach to covering security, compliance & resilience requirements that span multiple laws, regulations and frameworks.

SCR CAP Body of Knowledge (SCR CAP BoK)

The gain an understanding of what the SCR CAP is and how to get SCF certified, start with the SCR CAP Body of Knowledge (SCR CAP BoK), since it is the authoritative source for the SCR CAP.[50]



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.[51] 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.

[49] *SCR CAP - https://securecontrolsframework.com/training-certifications/scf-certifications/scf-conformity-assessment-program-cap/*

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

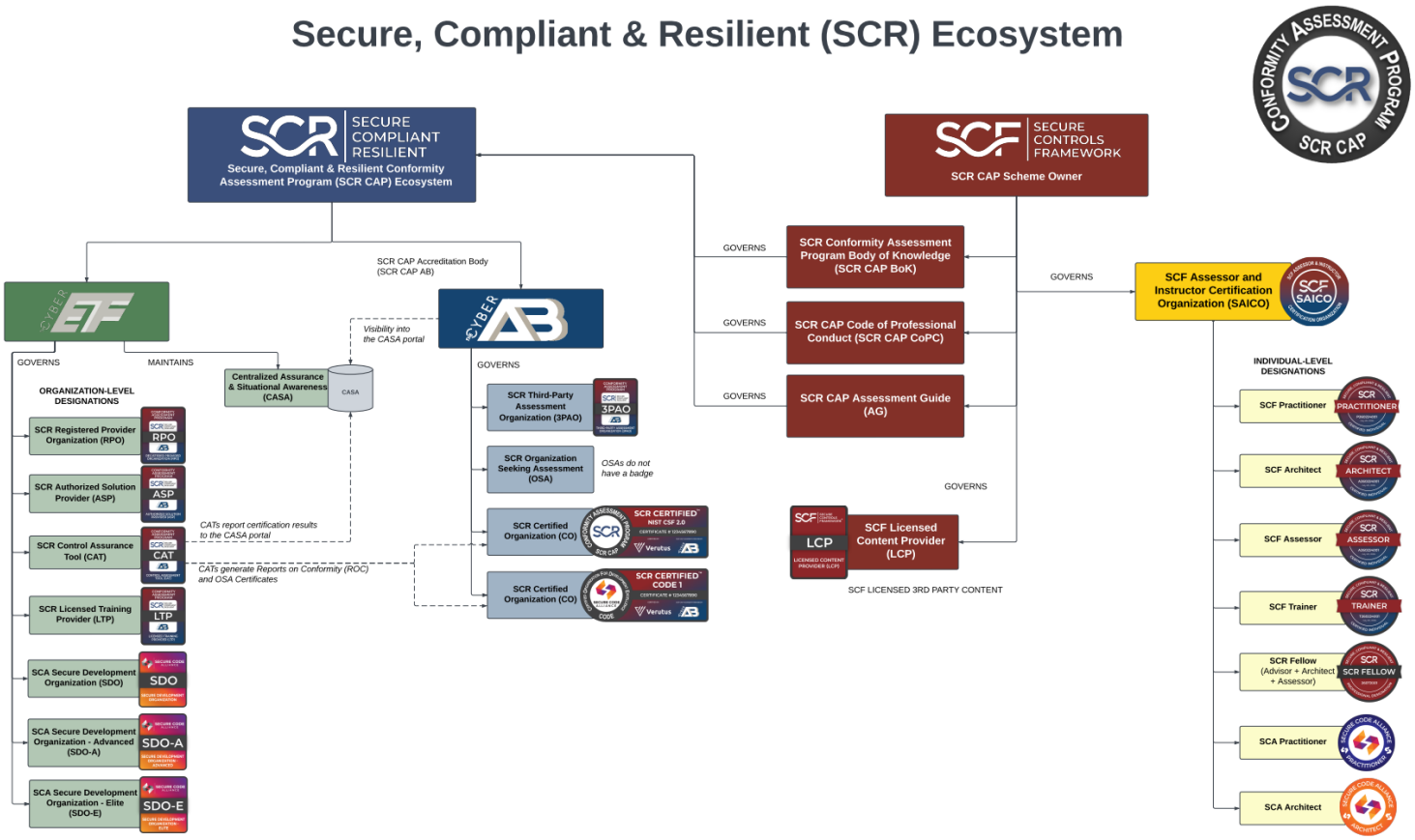
[51] *NIST SP 2000-01 - https://www.nist.gov/publications/abcs-conformity-assessment*

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SCR CAP Ecosystem

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



The Cyber AB & Cyber EF

The Cyber AB and Cyber EF govern the following aspects of the SCR CAP Ecosystem:

- **SCR Third-Party Assessment Organization (SCR 3PAO).** SCR 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 SCR 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. SCR 3PAOs play a critical role in maintaining the integrity and credibility of SCF certifications through rigorous and impartial assessments.
- **SCR Control Assurance Tool (SCR CAT).** SCR CATs are Governance, Risk, and Compliance (GRC) platforms that specialize in integrating the SCF framework. SCR CATs facilitate seamless integration, accurate compliance interpretation, and structured risk management to ensure GRC tools effectively operationalize SCF compliance. By embedding SCR CAP best practices into data, risk, and compliance management workflows, SCR CATs reinforce a structured and scalable approach to SCF implementation within GRC environments, enhancing organizations' ability to manage risk and ensure cross-regulatory compliance effectively.
- **SCR Authorized Solutions Provider (SCR ASP).** SCR 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. SCR 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.
- **SCR Registered Provider Organization (SCR RPO).** SCR RPOs are organizations that provide SCF-related professional services, including consulting and implementation. SCR RPOs assist organizations in preparing for assessments, streamlining SCF adoption, and ensuring alignment with cybersecurity and compliance objectives. SCR RPOs have demonstrated a commitment to professionalism and expertise in implementing the SCF within diverse business environments.
- **SCR Organizations Seeking Assessment (SCR OSA).** SCR OSAs are organizations that are working towards earning a

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

SCF-based certification but have not yet undergone a SCR CAP conformity assessment.

- **SCR Certified Organization (SCR CO).** SCF COs are SCR OSA that have successfully passed an SCR 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 SCR CAP Ecosystem. SCF COs maintain their certification through ongoing compliance efforts, periodic assessments, and adherence to SCF standards.

SCR Assessor and Instructor Certification Organization (SAICO)

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

- **SCR Practitioner.** SCR 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 security, compliance & resilience program.
- **SCR Architect.** SCR Architects are SAICO-certified individuals who have advanced SCF-related knowledge and competence necessary to (1) Architect and design SCF-based security, compliance & resilience 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-AI) considerations; (2) Assist SCR Practitioners with the implementation of SCF controls; and (3) Make adjustments to the security, compliance & resilience programs to account for new and/or changed laws, regulations and frameworks that affect the PPTDF-AI.
- **SCR Assessor.** SCR 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 SCR Conformity Assessment Program (SCR 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).
- **SCR Licensed Training Provider (SCR LTP).** SCR LTPs are SAICO-certified organizations that deliver a SAICO-approved individual-level certification training program using SCR Trainers.
- **SCR Trainer.** SCR Trainers are SAICO-certified individuals responsible for delivering initial and recurring SCF-based educational training for SAICO-approved individual-level certifications.

The SCF Council

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

- **SCR CAP Body of Knowledge (SCR CAP BoK).** SCR CAP BoK describes SCR CAP-related 3PAAC activities.
- **SCR 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Section 19. SCF Training & Individual Certifications

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

SCR Practitioner

SCR Practitioners are certified individuals who have the knowledge and skills to: [52]

1. implement SCF controls that align with the SCF recommended practices and structure; and
2. maintain an organization's security, compliance & resilience program.

SCR Architect

SCR Architects are certified individuals who have the knowledge and skills to design SCF-based security, compliance & resilience 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-AI) considerations. [53]

SCR Assessor

SCR 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 (SCR CAP). [54]

SCR Trainer

SCR Trainers are certified individuals who work for a SCF Licensed Training Provider (LTP) to perform SCF-approved training. The SCR Trainer role is expected to be available in 2027.

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

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

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

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

Section 20. Frequently Asked Questions (FAQ)

The SCF is more than just an assortment of security, compliance and resilience 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 security, compliance & resilience 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. Sign up for the SCF Discord server to ask questions;
2. Hire a SCR Trainer from the SCF Marketplace to provide individual or group training; and/or
3. Hire a SCR Practitioner or SCR Architect from the SCF Marketplace to get 1-1 consulting expertise.

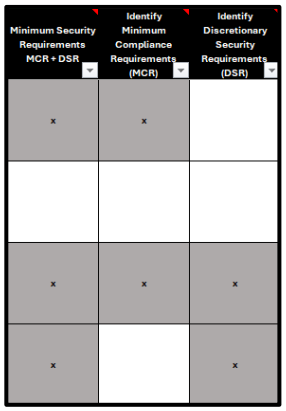
While the SCF Council gives away the SCF for free, if you want a consultant to take you through setting up or operationalizing your control set, you will have to pay for that service. The SCF Marketplace has a non-exclusive listing of security, compliance and resilience professionals who have the skills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



© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 security, compliance and resilience 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 security, compliance and resilience 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 SCR 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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

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 security, compliance & resilience-related Third-Party Assessment, Attestation and Certification Services (3PAAC Services). By following the Cybersecurity & Data Protection Assessment Standards (CDPAS) approach, security, compliance & resilience 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 SCR CAP.

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

The SCR Conformity Assessment Program (SCR CAP) is an organization-level conformity assessment. The SCR CAP is designed to utilize tailored security, compliance and resilience 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 security, compliance and resilience-specific laws, regulations and frameworks.

The SCR 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 SCR CAP is unique in its metaframework approach to covering security, compliance & resilience 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.

© 2026. Secure Controls Framework Council, LLC. All Rights Reserved.

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