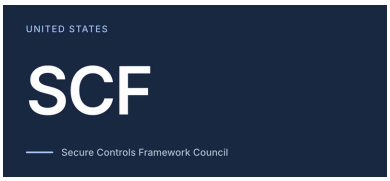
SmartSuite

Framework / Cybersecurity / Other

Secure Controls Framework (SCF)

The Secure Controls Framework (SCF) is a free CC BY-ND 4.0 control catalog of 1,500+ controls in 34 domains, mapped with STRM to over 250 laws, regulations and frameworks.



What it is

The Secure Controls Framework (SCF) is a free cybersecurity and data privacy control catalog, published by the Secure Controls Framework Council, LLC under a Creative Commons Attribution-NoDerivatives 4.0 International license, that organizations use as one common control set in place of separate control lists for each law, regulation and standard they must meet. The SCF Council describes it as a metaframework: more than 1,500 controls in 34 domains, each mapped to the requirements of over 250 laws, regulations and frameworks, released quarterly with the current release being the 2026 Q3 release of September 21, 2026.

At a glance

PUBLISHER
Secure Controls Framework Council, LLC

TYPE
Control Framework

VERSION
2026 Q3 release (September 21, 2026): 1,500+ controls in 34 domains; released quarterly

EFFECTIVE
September 21, 2026 (2026 Q3 release; the prior release, 2026.2, dated July 7, 2026)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States (used globally)

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
High

Source: securecontrolsframework.com/

Why it matters

- **One control set, many obligations** More than 1,500 controls in 34 domains carry STRM crosswalks to over 250 laws, regulations and frameworks, so one implemented control serves every regime that maps to it.
- **Transparent mappings** Since the 2024 releases every crosswalk uses Set Theory Relationship Mapping based on NIST IR 8477: each mapping states whether the SCF control is a subset of, equal to, a superset of, intersects with or has no relationship to the external requirement, with a strength score.
- **Built-in maturity criteria** The SCR-CMM gives each control criteria for six levels, from Level 0 (Not Performed) to Level 5 (Continuously Improving), so target and actual maturity can be scored per control.
- **Free and machine-readable** Released at no cost under CC BY-ND 4.0 in Excel/CSV and JSON (NIST OSCAL), with a legacy-to-current control number mapping carried inside the catalog after the 2026 Q3 renumbering.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports SCF

SCF Control Library

Hold the 34 domains and 1,500+ controls as records with domain code, control number, legacy number and owner, updated when a quarterly release lands.

STRM Crosswalk Register

Link each control to the external clauses it maps to, with the relationship type (Subset Of, Equal To, Superset Of, Intersects With) and strength score, so every obligation shows its covering controls.

SCR-CMM Maturity Scoring

Record target and current maturity (Level 0 to 5) per control and report the gap by domain and by mapped framework.

Risk and Threat Catalog

Track the SCF risk and threat entries against controls in Cyber & IT Risk, with the Likely, Possible or Unlikely rating and the treatment decision.

Evidence and Compensating Controls

Attach evidence to each control once and reuse it across regimes; record any compensating control chosen from the SCF list with its justification.

SCR CAP Readiness

Run the self-assessment that precedes a third-party SCR CAP assessment as a project: statement of applicability, boundary, findings and remediation tasks for the accredited assessor.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | ISO 27001:2022 | ISO 27002:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

Secure Controls Framework Specification

Defines a comprehensive set of cybersecurity and data protection controls to address various regulations.

securecontrolsframework.com

SCF Implementation Guide

Provides guidance to assist organizations in implementing the Secure Controls Framework effectively.

securecontrolsframework.com/free-content/prioritized-implementation-guide-pig

SCF Control Catalog

Outlines all controls included in the Secure Controls Framework for comprehensive security management.

securecontrolsframework.com/free-content/scf-download

SCF Capability Maturity Model (SCR-CMM)

The six-level maturity model that scores every SCF control, built on the SSE-CMM v2.0 structure.

securecontrolsframework.com/free-content/capability-maturity-model-scr-cmm

Frequently asked questions

What is the Secure Controls Framework and who publishes it?

The SCF is a free catalog of more than 1,500 cybersecurity and data privacy controls in 34 domains, published by the Secure Controls Framework Council, LLC under a Creative Commons Attribution-NoDerivatives 4.0 International license. The Council calls it a metaframework because each control is mapped to the requirements of over 250 laws, regulations and frameworks, so one control set can serve many obligations.

How does Set Theory Relationship Mapping (STRM) work in the SCF?

STRM follows NIST IR 8477. For each pairing of an SCF control with an external clause, the mapping records one of five relationship types (Subset Of, Equal To, Superset Of, Intersects With or No Relationship) and a numeric strength score. Since the 2026.2 release of July 7, 2026 every mapped framework has published STRM except the deprecated NIST SP 800-53 Rev. 4 and the SIG, whose mappings come from its own publisher.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the SCR-CMM maturity levels?

The Secure, Compliant & Resilient Capability Maturity Model is built on the SSE-CMM v2.0 structure and gives every control criteria for six levels: Level 0 Not Performed, Level 1 Performed Informally, Level 2 Planned & Tracked, Level 3 Well Defined, Level 4 Quantitatively Controlled and Level 5 Continuously Improving. Each succeeding level builds on its predecessor, and the model measures maturity rather than the rigor of the control.

What changed in the 2026 releases of the SCF?

The 2026.1 release of April 1, 2026 added and updated STRM mappings and maturity criteria. The 2026.2 release of July 7, 2026 added the Quantum Security (QTS) domain, completed STRM for the mapped frameworks and added lists of compensating controls. The 2026 Q3 release of September 21, 2026 renumbered most controls, kept a current-to-legacy mapping inside the catalog, extended the mappings to over 250 laws, regulations and frameworks and rated every risk and threat catalog entry against controls as Likely, Possible or Unlikely.

Can an organization be certified against the SCF?

Yes, through the Secure, Compliant & Resilient Conformity Assessment Program (SCR CAP), for which the Cyber AB is the accreditation body. Accredited third-party assessment organizations assess the organization with an examine, interview and test methodology against an SCF-based control set, such as NIST CSF 2.0, NY DFS 23 NYCRR Part 500, CMMC Level 1, the HIPAA Security Rule, NIST SP 800-171 R3 or SCF CORE Fundamentals, leading to an SCF Certified designation. Use of the catalog itself needs no certification.

License included / downloadable: Yes The SCF catalog, its STRM crosswalks in PDF form and the supporting models are free downloads from the Secure Controls Framework Council under the Creative Commons Attribution-NoDerivatives 4.0 International license; editable Excel versions of the STRM mappings are sold separately.

Full framework page and mappings: smartsuite.com/frameworks/secure-controls-framework-scf