axiom
corestream grc

The Secure Controls Framework and why it matters for compliance

Why do compliance teams need a better way to manage overlapping frameworks?

Most organizations are not managing 1 compliance obligation. They are managing several at once.

A business may need to show alignment with several frameworks including;

- ISO 27001 for security management,
- SOC 2 for customer assurance,
- GDPR for personal data protection,
- DORA for operational resilience,
- NIS2 for cybersecurity obligations, and
- internal control requirements from customers, regulators, or contractual commitments.

The problem is that these obligations often **ask similar questions in different ways.**

For example, many of the above frameworks require an organization to prove that access **rights are reviewed, risks are assessed, vendors are monitored, incidents are managed, and evidence is retained.** But if each framework is assessed separately, the same control can be tested, documented, and reported several times.

That creates wasted work.

It also creates risk. If different teams interpret the same control differently, compliance reporting can become fragmented. Evidence sits in different places. Owners are unclear. Remediation is tracked manually. Leaders get reports, but not always a reliable view of the underlying control position.

The Secure Controls Framework was created to solve this exact problem.

Rather than forcing teams to manage every framework in isolation, SCF normalizes overlapping requirements into a common control architecture. That gives compliance, risk, security, audit, and privacy teams a **clearer way to understand which obligations align, which evidence can be reused, and where real gaps remain.**

What is the Secure Controls Framework?

The **Secure Controls Framework** is a free cybersecurity and data privacy metaframework.

It is **built and maintained by a volunteer community of cybersecurity and GRC professionals,** including CISOs, architects, engineers, auditors, privacy experts, and consultants.

Its purpose is to help organizations **build secure, compliant, and resilient capabilities** in a more efficient and cost-effective way.

SCF is designed as a Common Controls Framework. That means it gives organizations 1 shared control structure that can be mapped across multiple statutory, regulatory, and contractual requirements.

Within the SCF framework there are:

- 1,400+ controls
- 33 domains
- 200+ laws, regulations and frameworks
- 5 geographic regions, including General, USA, EMEA, APAC and Americas

The important point is this: SCF is not just another framework to add to the workload.

It is designed to **reduce the workload** created by too many **overlapping frameworks.**

"The SCF makes compliance a natural byproduct of secure and resilient practices. It is the world's most comprehensive cybersecurity and data privacy metaframework."

Tom Cornelius, Co-Founder

SCF SECURE CONTROLS FRAMEWORK

Why does SCF matter for multi-framework compliance?

Multi-framework compliance is where duplication becomes most painful.

If a team assesses **ISO 27001, DORA, NIS2, SOC 2, and GDPR** separately, they may end up testing similar controls several times. That can mean multiple evidence requests, multiple spreadsheets, multiple owner follow-ups, and multiple versions of the same control story.

SCF helps prevent this by making control overlap visible.

In practice, that means teams can use 1 control architecture to understand:

- Where obligations align
- Where evidence can be reused
- Where a control only partially meets a requirement
- Where genuine gaps remain
- Which controls support multiple frameworks

This is the shift from “complete another framework assessment” to **“understand our control coverage across the business.”**

That distinction matters.

A framework-by-framework approach can create activity without clarity. In contrast, a common control approach helps teams see how the same control supports multiple obligations, and where the organization still needs to improve.

SCF is also designed as a **living control set.** It is updated as laws change, new frameworks emerge, and threat landscapes evolve.

That is important because compliance is not static. Regulations change. Customer expectations change. New technology risks emerge. Vendor environments shift. A control architecture that does not stay current quickly becomes another manual maintenance burden.

How does SCF make compliance mapping more defensible?

Framework mapping is only useful if it can **stand up to challenge.**

A weak crosswalk can create false confidence. That is especially risky where a control only partially satisfies a requirement, or where a team assumes that 1 piece of evidence proves more than it really does.

SCF addresses this by using **NIST IR 8477 Set Theory Relationship Mapping, known as STRM**. SCF states that this approach supports **more rigorous mapping by documenting the relationship type and strength between controls and requirements.**

"This is the US Government's gold standard for crosswalk mapping. Every mapping documents a precise relationship type and strength score, making coverage defensible and auditable."

That matters because GRC teams need to explain more than whether a control exists.

They need to explain:

- Which **obligations** the control supports
- How strong the **relationship** is
- Whether the **requirement** is fully or partially met
- What **evidence** proves the control is operating
- Who owns the **control**
- What **remediation** is underway if the control is weak

SCF also participates in the NIST National Online Informative References Program, or **OLIR**. NIST describes OLIR as;

"A NIST 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"

SCF states that NIST accepted its submitted Online Informative References for both NIST CSF v1.1 and NIST SP 800-171 R2. In practice, this gives organizations a stronger reference point when using SCF to understand how their controls align with NIST requirements.

That matters because defensible compliance is not just about saying, "we mapped this framework."

Teams **need to show how the mapping was done, what each control is intended to cover, and where the relationship between a control and a requirement is strong, partial, or limited.** This gives auditors, customers, and internal stakeholders a clearer basis for reviewing control coverage.

"The challenge for GRC teams is no longer whether they can produce another compliance report. It is whether they can prove, quickly and defensibly, how controls map to real obligations across the business.

SCF gives organizations a stronger control architecture, but the real value comes when that architecture is connected to evidence, ownership, workflow, and reporting. That is where compliance moves from one-off / periodic audits to a live assurance model."

Paul Cadwallader, GRC Strategy Director

corestream grc

Where does AI-enabled GRC fit into SCF?

SCF provides the **control architecture.**

But it does not run the compliance process by itself.

Teams still need to **gather evidence, map obligations, assign owners, review gaps, manage remediation, and report to boards, auditors, regulators, and customers.**

That is where **AI-enabled GRC can help.**

But in compliance, AI cannot just produce a plausible answer. It has to produce an answer that can be **checked, evidenced, reviewed, owned, and defended.**

This is why CoreStream GRC partnered with SANNOS.

SANNOS AI has been tested against 3,000+ pages of SCF compliance documentation with 0 false positives.

The value is not simply that AI can work faster.

The value is that AI can help structure evidence, identify gaps, and support mapping in a way that remains traceable.

That matters because compliance teams do not need another black box. They need **outputs that can survive audit review.**

With SANNOS, the AI output is designed to be:

- Structured
- Traceable
- Reviewable
- Defensible

SANNOS.

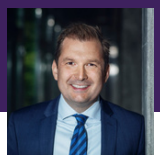
5.0 Where does AI-enabled GRC fit into SCF?

That is the difference between AI-assisted compliance and AI-assured compliance.

"In compliance and assurance, speed only matters if the output is trusted and audit-defensible. SCF provides organizations with a strong common control language, but real AI assurance must go beyond document summaries and policy search. It must understand controls, validate evidence, identify gaps, and produce outputs that withstand audit and regulatory scrutiny.

That is the difference between AI-assisted compliance and AI-assured compliance. SANNOS is currently the only AI platform certified by the Cyber AB within the SCF ecosystem."

Anders Søborg, CEO



SANNOS.

CoreStream GRC powered by SANNOS AI is built around this **"assess once, map many" model.**

The results of this partnership are drastic. B**aseline assessment timelines can be reduced from 2 to 4 months to 2 to 4 weeks, with 60 to 80% cost reduction and 75% timeline reduction compared with traditional multi-framework compliance delivery.**

The goal is not to remove human judgment.

The goal is to **remove the manual repetition that stops skilled teams from focusing on risk, gaps, ownership, and improvement.**

Want to learn more about this partnership?

Learn more

How can SCF support third-party risk management?

T**hird-party risk** is one of the clearest use cases for SCF.

A single critical supplier can create obligations across cybersecurity, data privacy, operational resilience, contractual compliance, regulatory reporting, and customer assurance.

For example, a **vendor may need to be assessed against requirements linked to DORA, NIS2, ISO 27001, SOC 2, GDPR, and internal customer assurance controls.**

Without a common control structure, third-party risk teams can end up running separate assessments for overlapping requirements. Vendors get asked for the same evidence in different formats. Internal teams spend time reconciling answers. Risk owners struggle to compare results across suppliers.

SCF gives third-party risk teams a common control language.

AI-enabled GRC can then help turn that control language into **faster intake, risk scoring, contract review, and re-assessment.**

6.0 How can SCF support third-party risk management?

CoreStream GRC powered by SANNOS AI can support third-party risk workflows including:

- Automated vendor intake
- AI risk scoring
- Contract review
- Continuous re-assessment
- Assessment across 100+ vendors simultaneously

That is where SCF becomes more than a framework reference.

It becomes **part of a live third-party risk management process.**

Want to learn more about our third-party risk management capabilities?

SCF x SANNOS AI datasheet

How should organizations evaluate SCF-enabled GRC software?

The real test is not whether a platform says it supports SCF.

The real test is whether it can **turn SCF mapping into usable assurance, in the way the business actually works.**

A useful starting question is:
Can the platform help your team **assess once, reuse the result across multiple frameworks, and keep the supporting evidence, ownership, workflow, hosting, and reporting connected?**

That question quickly separates surface-level framework support from **practical GRC value.**

7.0 How should organizations evaluate SCF-enabled GRC software?

When evaluating SCF-enabled GRC software, organizations should ask:

- Can the platform **map 1 control to multiple obligations?**
- Can it **show how each control links to each framework?**
- Can it explain **whether the relationship is full, partial, or limited?**
- Can it **flex to the organization's existing workflows, terminology, approval routes, and reporting needs?**
- Can it **support specific data hosting requirements across regions, cloud, or on-premises environments?**
- Can **evidence be traced to source systems, documents, or owners?**
- Can it **integrate** with the tools the business already uses, rather than forcing teams into another disconnected process?
- Can **humans review, approve, and challenge AI-generated outputs?**
- Can **third-party risk, control testing, remediation, and reporting sit in 1 connected process?**
- Can the platform support **live dashboards rather than static compliance reports?**
- Can it be **configured as requirements change, without creating unnecessary complexity?**
- Can **outputs be used by auditors, boards, regulators, and customers?**

These questions matter because compliance teams do not need another tool that simply stores framework content.

They need a **connected assurance process** that fits how their organization operates, supports the data and hosting requirements they have to meet, and helps them **prove what is working, what is missing, and what needs to happen next.**

What does continuous compliance actually mean?

SCF gives organizations the control architecture. CoreStream GRC powered by SANNOS AI turns that architecture into a **live compliance process.**

That is the important distinction.

A static controls library can help teams understand overlap. But on its own, it does not collect evidence, route approvals, assign remediation, manage third-party assessments, or show leaders where compliance gaps sit today.

CoreStream GRC powered by SANNOS AI is designed to **connect SCF mapping to the practical work of GRC**, including assessment, evidence, ownership, workflow, reporting, remediation, and audit readiness.

The combined approach supports 3 practical solution areas:

- **Baseline assessments delivered in 2 to 4 weeks**
- **Third-party risk management across 100+ vendors simultaneously**
- **Secure Controls Framework mapping for multi-framework continuous compliance**

The value is not just faster assessment.

It is a **better way to operate compliance across multiple frameworks**. Teams can **assess once, reuse control knowledge across many obligations, validate AI-supported outputs, and keep a clear line of sight from requirement to control, evidence, owner, gap, and action.**

That is where CoreStream GRC's flexibility matters. The platform can be configured around the organization's existing workflows, terminology, approval routes, reporting needs, integrations, and data hosting requirements, rather than forcing teams into a rigid process.

For compliance leaders, that means SCF does not sit in isolation as another reference framework. It becomes part of a **connected assurance model that can support internal control reviews, third-party risk assessments, board reporting, customer assurance, audit preparation, and regulatory response.**

The real outcome is not more documentation.

It is a **live, defensible view of compliance that shows what is covered, what is evidenced, what needs attention, and who owns the next step.**

Conclusion: SCF is not just another framework

The Secure Controls Framework matters because it reflects where compliance is going.

Organizations need a **clearer** way to manage overlapping obligations, prove control coverage, reuse evidence, and stay current as requirements change.

SCF helps by creating a **common control architecture.**

But the real value comes when that architecture is **connected to day-to-day GRC work.**

That means **evidence. Ownership. Workflow. Review. Remediation. Reporting. Audit trail**s.

For GRC leaders, the message is simple.

The future of compliance is not more framework-by-framework activity.

It is a **more connected, defensible, and continuous model of assurance.**

CoreStream GRC powered by SANNOS AI helps organizations move toward that model by bringing **SCF mapping into live GRC workflows, reducing manual effort, and helping teams build audit-ready outputs they can trust.**

Want to understand how SCF could support your multi-framework compliance program?

axiom
corestream grc

For more information please contact:

Email us to book your demo:
demo@corestreamgrc.com

corestreamgrc.com

Book a workshop

Book a demo

Follow us on LinkedIn