SECURITY, COMPLIANCE & RESILIENCE MANAGEMENT SYSTEM

A Defensible Governance Model for Security, Compliance & Resilience

https://securecontrolsframework.com

Cybersecurity: A Protracted War On An Asymmetric Battlefield

Security + Compliance + Resilience is a unified objective. With this multi-discipline approach to cybersecurity and data protection, it signals that an organization isn't just protected, but also meets its compliance requirements and can quickly bounce back from incidents.

The Security, Compliance & Resilience Management System (SCRMS) has two goals:

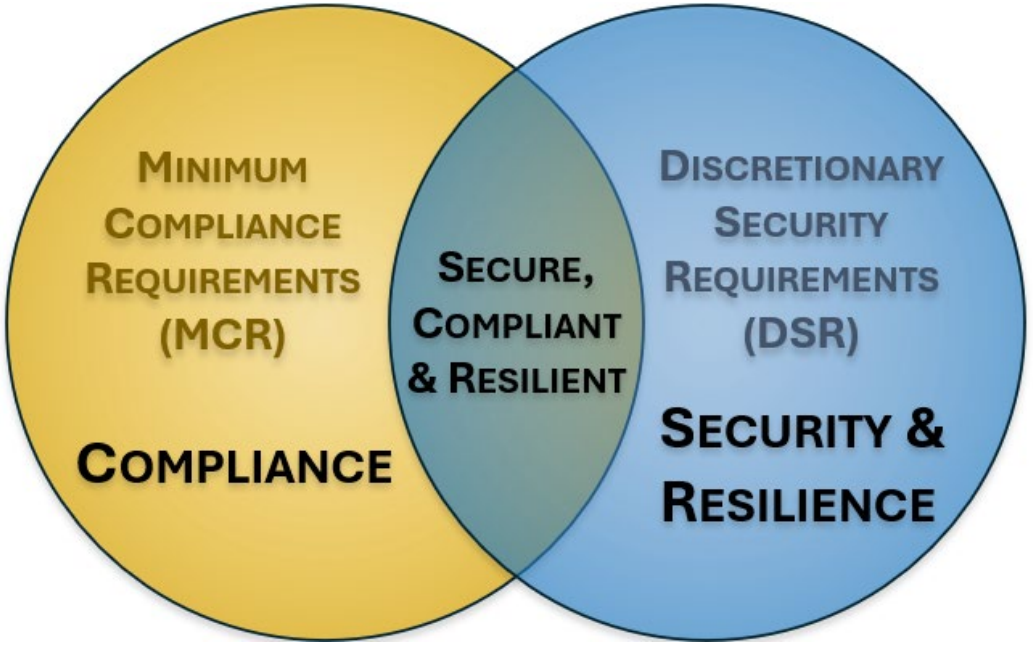
1. **Minimize an entity's attack surface.**
2. **Provide "defensible evidence" of reasonable practices.**

SCRMS is an operational assurance model

Minimize The Attack Surface

Minimizing an organization's attack surface must address more than just technical threats. This process involves defining a **Living Control Set (LCS)** that defines **Minimum Security Requirements (MSR)** necessary to be secure, compliant and resilient:

- **Minimum Compliance Requirements (MCR)** are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR focuses on compliance.
- **Discretionary Security Requirements (DSR)** are based on the organization's respective industry expectations and risk tolerance. DSR focuses on security and resilience.



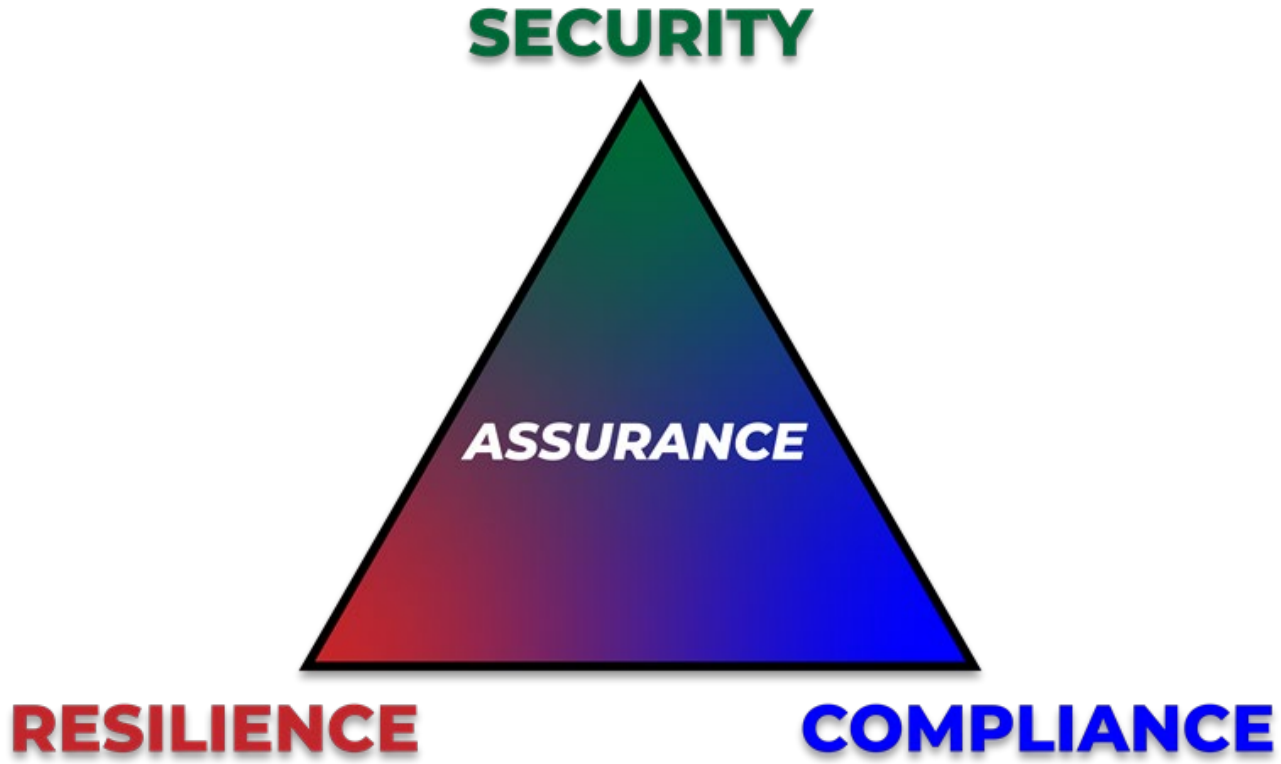
Defensible Evidence Focuses On What You Can Prove

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

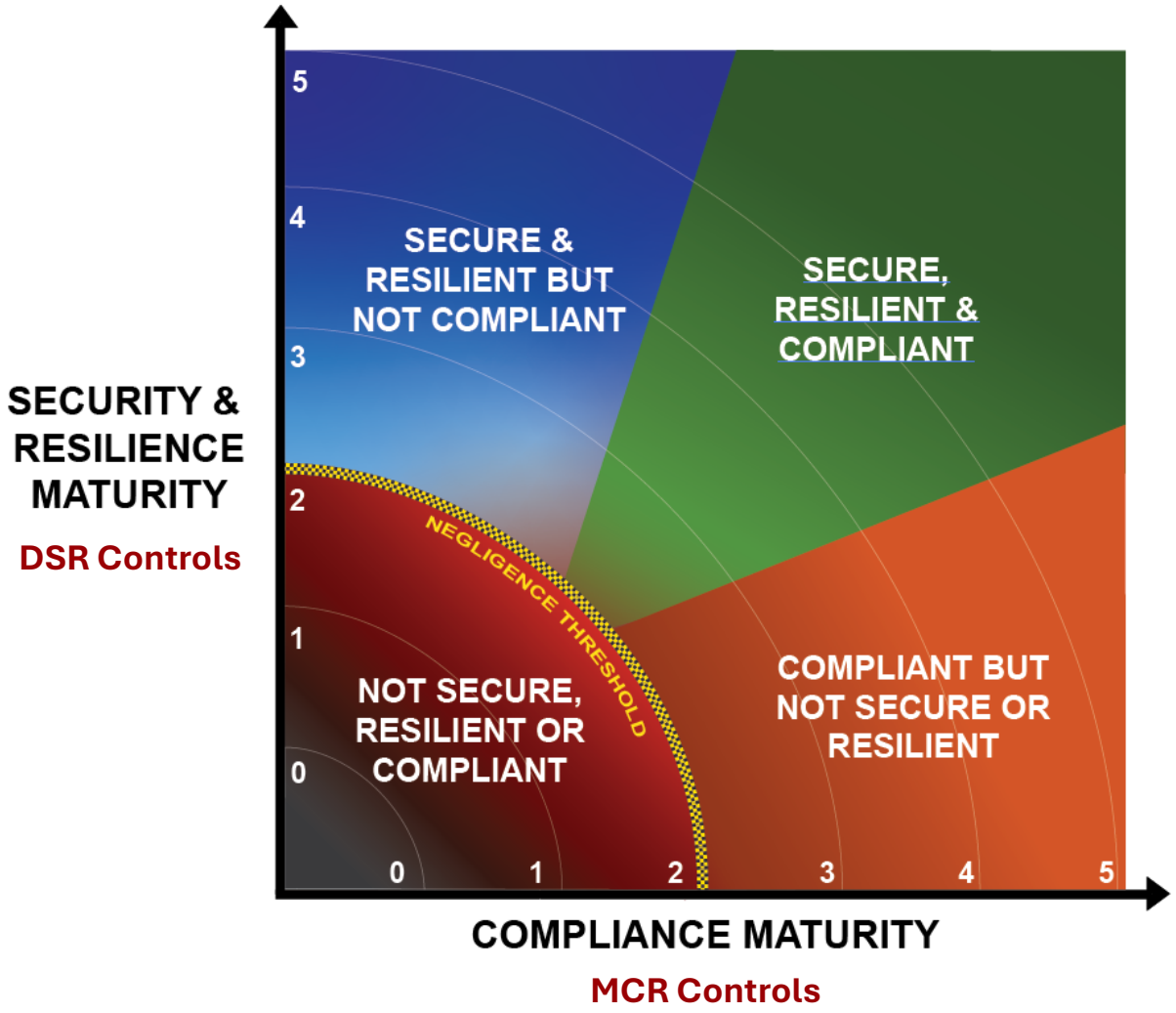
- Actually occurred.
- Were effective.
- Can withstand external scrutiny.

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

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



SCRMS: Framework-Agnostic Approach To A Governance Model



The SCRMS is a holistic, technology-agnostic approach to cybersecurity and data protection controls.

- Used to identify, implement and manage secure, compliant and resilient capabilities.
- Covers an organization's People, Processes, Technologies, Data and Facilities (PPTDF), regardless of how or where data is stored, processed and/or transmitted.

Bottom Line For Cybersecurity Leadership

Cybersecurity leadership operates in a world of regulators, class action lawsuits, AI risk, supply chain fragility and board scrutiny:

- SCRMS is not just an alternative to an audit management system (e.g., ISMS), but it's the logical successor.
- Defensible evidence is the design outcome.
- Compliance becomes a byproduct of secure and resilient operations, not the goal.

ISO 27001, SOC 2 & CMMC Answer:

"Can we pass an audit?"

SCRMS Answers:

"Can we prove we acted reasonably, responsibly and defensibly when it mattered most?"

The SCRMS Difference: Built for Reality, Not Just Audits

SCRMS replaces siloed management systems with a single, integrated governance model that aligns security, compliance, and resilience with real business risk.

SCRMS is designed to:

- Support executive and board decision-making.
- Reduce negligence exposure.
- Scale without excessive overhead.
- Address modern risks (e.g., AI, privacy, supply chain, etc.) by design.

Unlike other management system models, SCRMS:

- Distinguishes compliance from security.
- Prioritizes controls based on material risk.
- Aligns cybersecurity with enterprise risk management.

Value proposition is “comprehensive coverage” made up of security, compliance & resilience capabilities.

The Limits of The Traditional ISMS Model

The ISO-based **Information Security Management System (ISMS)** was primarily designed to:

- Demonstrate conformity to a single standard (e.g., ISO 27001); and
- Support certification through point-in-time audits.

ISMS was not designed to:

- Weigh controls differently, based on applicable threats and risks.
- Holistically look at the entire organization.
- Demonstrate due diligence and due care in litigation proceedings (beyond the scope of ISO 27001).
- Integrate AI, privacy, supply chain and resilience risk into a single management system.

Most organizations invest heavily in cybersecurity, yet still struggle to answer:

- *“Are we actually secure?”*
- *“Are we exposed to regulatory or legal risk?”*
- *“Can we defend our decisions for selecting security, compliance and resilience controls?”*

Traditional ISMS and certification-centric approaches focus on audits, not outcomes.

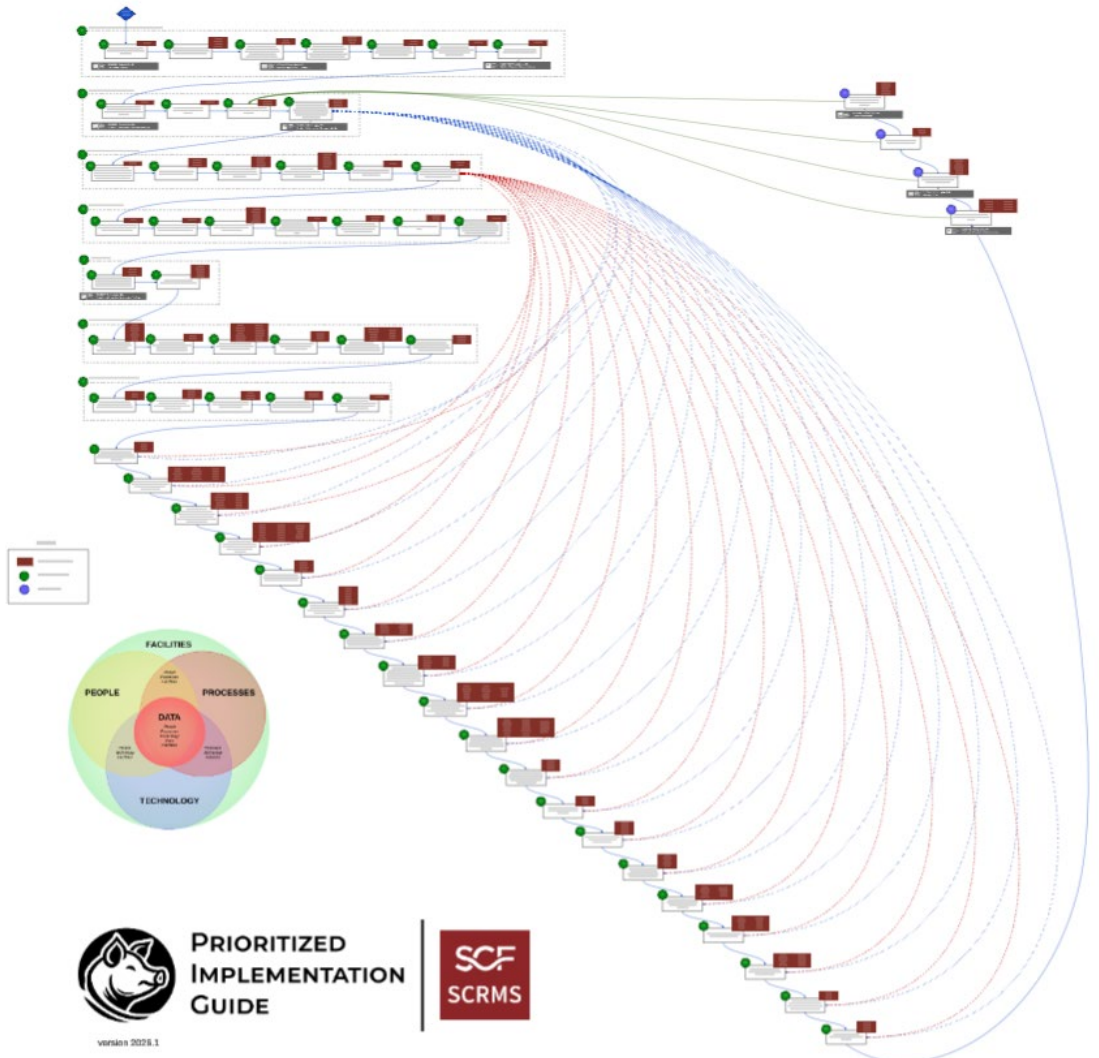
Core Philosophical Differences: ISMS vs SCRMS

Modern enterprises now operate in an environment defined by regulatory convergence, AI risk, supply chain dependency, litigation exposure, and board-level accountability.

SCRMS was purpose-built to address these realities by replacing siloed management systems with a **holistic, legally defensible and risk-driven governance model** that aligns cybersecurity directly with business operations.

Topic	ISO 27001 ISMS	SCRMS
Primary Objective	Certification conformity	Defensible practices
Governance Model	Single-domain (information security)	Integrated disciplines (security, compliance & resilience)
Risk Perspective	Abstract risk assessment	Nested, decision-grade risk management
Success Metric	Passing audits	Demonstrating conformity, withstanding external scrutiny and withstanding incidents
Evolution Model	Add-on management systems	Unified, extensible architecture

SCRMS Prioritized Implementation Plan (SCRMS-PIG)



The SCRMS comes with a practitioner-focused guidebook to implement a prioritized rollout of capabilities.

This guide breaks the SCRMS down into 30 steps:

- 26 steps focused on due diligence.
- 4 steps focused on due care.

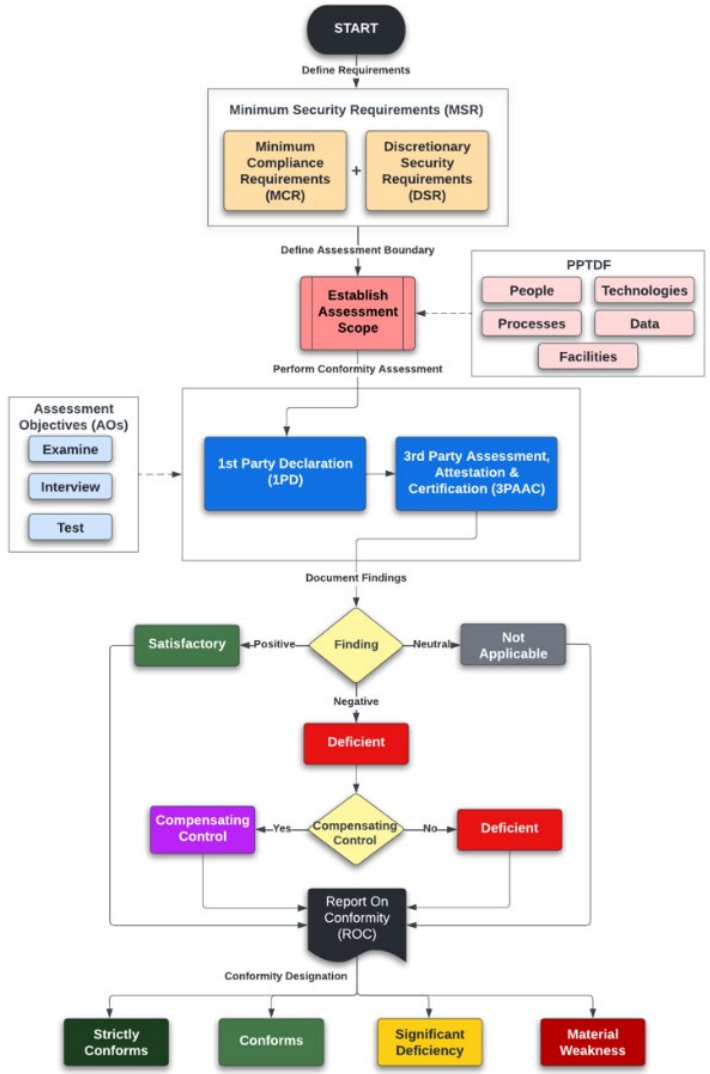
The SCRMS-PIG can be used to create a project plan for implementation purposes.

Demonstrating Assurance To Stakeholders

The SCF has an assurance mechanism, the Security, Compliance & Resilience Conformity Assessment Program (SCR CAP).

The SCR CAP is an organization-level conformity assessment that is designed to utilize tailored cybersecurity and privacy controls that specifically address the applicable security, compliance and resilience requirements.

By using the metaframework nature of the SCF, an entity can perform a conformity assessment that spans multiple cybersecurity and data privacy-specific laws, regulations and frameworks.



SCRMS Is Designed for Defensibility, Not Certification Theater

Cybersecurity Leadership Takeaway #1

The SCRMS prepares you to survive class action lawsuits, regulators and insurer investigations. Certifications only prepare you for auditors.

ISO 27001, SOC 2 & CMMC Reality

- Certification ≠ due care.
- Courts and regulators rarely accept *"we were XYZ-certified"* as a defense.

SCRMS Advantage

- Explicit negligence threshold modeling.
- Evidence is preserved with litigation utility in mind.
- Risk-based prioritization drives funding and sequencing.
- Defensible governance becomes an input to business planning, not an afterthought.

SCRMS Accepts That Not All Controls Are Equal

Cybersecurity Leadership Takeaway #2

The SCRMS acknowledges the reality that some failures are existential.

ISO 27001, SOC 2 & CMMC Reality

- All controls appear conceptually equivalent.
- Limited notion of material controls.

SCRMS Advantage

- Material controls cannot be dismissed through compensating controls;
- Explicit distinction between:
  - Compliance floor with Minimum Compliance Requirements (MCR); and
  - Security optimization with Discretionary Security Requirements (DSR).
- Maturity targets are economically justified.

SCRMS Reflects How Risk Actually Works

Cybersecurity Leadership Takeaway #3

The SCRMS treats risk as a *decision system*, not a compliance exercise.

ISO 27001, SOC 2 & CMMC Reality

- Risk assessment is often abstract.
- Risk appetite is rarely enforced operationally.
- Controls exist independently of materiality.

SCRMS Advantage

- Nested risk model: Enterprise Risk Management (ERM) > Cybersecurity & Data Protection Risk Management (CDPRM) > Third-Party Risk Management (TPRM).
- Material risk, threat, control and incident concepts are explicit and measurable.
- Explicit linkages between:
  - Risk appetite;
  - Risk tolerance; and
  - Risk thresholds.

SCRMS Eliminates Management-System Sprawl

Cybersecurity Leadership Takeaway #4

The SCRMS reflects modern enterprises, not certification catalogs.

ISO 27001, SOC 2 & CMMC Reality

- ISMS + AIMS + PIMS + BCMS = governance fragmentation.
- Each system introduces new audits, documentation and overhead.

SCRMS Advantage

- Single integrated Security, Compliance & Resilience ecosystem.
- AI, privacy, supply chain and safety are native, not bolt-on concepts.
- Plan, Do, Check & Act (PDCA) applies holistically, not per standard.