SCF

SCF SCRMS

SECURITY, COMPLIANCE & RESILIANCE MANAGEMENT SYSTEM

Phased ISMS Transition Roadmap To SCRMS Adoption

https://securecontrolsframework.com

ISO 27001 to SCRMS Transition Roadmap

This example roadmap is designed for **organizations that already have an ISO 27001 ISMS** and want to evolve toward a SCF-based SCRMS **without breaking audits, contracts or board confidence**.

The SCRMS does not require abandoning ISO 27001 artifacts immediately. Instead, ISO deliverables are **absorbed, reclassified, and subordinated** within the SCRMS until those artifacts naturally become legacy compliance evidence.

This avoids:

- Audit disruption
- Contract violations
- Political resistance from entrenched stakeholders
- "Rip and replace" failures
- Consultant-driven reinvention
- Certification theater
- Control bloat

Phase 1: Foundation & Reframing (0-90 Days)

Objective: Reposition existing ISMS artifacts inside the SCRMS model

Risk Level: Low

Disruption: Minimal

Key Outcomes:

- The SCRMS established as the primary governance model.
- ISO 27001 is reframed as a compliance input.
- No changes to certification posture.

Phase Deliverables (reviewed & approved documentation)

- Charter that establishes the SCRMS.
- Documented Living Control Set (LCS) (generated from MCR & DSR).
- Organization-specific materiality criteria definitions (e.g., risks, threats, incidents and controls).

Phase 1: Foundation & Reframing (0-90 Days) (continued)

Action #1: Declare the SCRMS as the Governance Umbrella

- Executive memo or charter stating:
  - SCRMS governs security, compliance, and resilience.
  - ISO 27001 is treated as a Minimum Compliance Requirement (MCR) where applicable.
- Position this as a clarification, not a replacement.

Action #2: Map ISO Artifacts Into SCRMS Constructs

ISO 27001 Artifact	SCRMS Reclassification
ISMS Scope	SCRMS Scope & Context
Statement of Applicability	Minimum Security Requirements (MSR)
Risk Register	Risk Catalog
Controls Annex A	SCF-Mapped Controls
Internal Audit	Due Care / Conformity Activity

Phase 1: Foundation & Reframing (0-90 Days) (continued)

Action #3: Establish Minimum Security Requirements (MSR)

- Identify MSR components:
  - Minimum Compliance Requirements (MCR) (e.g., statutory, regulatory & contractual obligations)
  - Initial Discretionary Security Requirements (DSR) (e.g., known gaps ISO does not address well)
- MSR becomes the single authoritative control baseline

Action #4: Introduce Materiality Language

- Define (at a minimum):
  - What constitutes a material incident.
  - What constitutes a material control failure.
- This is often the first “*AHA!*” moment for leadership

Phase 2: Risk & Control Realignment (90-180 Days)

Objective: Shift from audit-centric to decision-centric security.

Risk Level: Medium

Disruption: Managed

Key Outcomes:

- Risk management begins driving priorities.
- Control maturity becomes selective and intentional.
- ISO audits continue uninterrupted.

Phase Deliverables (reviewed & approved documentation)

- Charter that aligns risk management across the organization (e.g., risk appetite, risk tolerance & risk thresholds).
- Catalog of material controls.
- Metrics that support the SCRMS.

Phase 2: Risk & Control Realignment (90-180 Days) (continued)

Action #5: Implement Nested Risk Management

- Align: Enterprise Risk Management (ERM) > Cybersecurity & Data Protection Risk Management (CDPRM) > Third-Party Risk Management (TPRM).
- Normalize: Risk appetite (board), Risk tolerance (operations) & Risk thresholds (execution).

This is where the SCRMS outperforms ISO from a holistic approach to security, compliance and resilience.

Action #6: Identify Material Controls

- Flag controls where:
  - No compensating controls are acceptable.
  - Failure would exceed materiality thresholds.
- These controls receive:
  - Higher maturity targets.
  - Priority funding.
  - Executive visibility.

Phase 2: Risk & Control Realignment (90-180 Days) (continued)

Action #7: Shift Metrics to Situational Awareness

- Move away from “vanity metrics (e.g., “% compliant” measurements).
- Adopt trend-based analytics that:
  - Tell the story of risk and threat management trends.
  - Track control effectiveness over time.

Leadership Question Becomes:

“Are we operating within our risk threshold?”

Phase 3: SCRMS-Native Operations (180–365 Days)

Objective: Make ISO optional and the SCRMS indispensable.

Risk Level: Low–Medium

Disruption: Strategic

Key Outcomes:

- The SCRMS is operationally dominant.
- ISO certifications becomes secondary or optional.
- The organization is defensible beyond audits.

Phase Deliverables (reviewed & approved documentation)

- Conformity assessment to validate defensible evidence.
- Plan of Action & Milestones (POA&M) to remediate deficiencies.
- Updated Living Control Set (LCS) to address evolving risks and threats to the organization.

Phase 3: SCRMS-Native Operations (180–365 Days) (continued)

Action #8: Embed SCRMS into Business Planning

- Security becomes input, not overhead. The SCRMS ties outputs to:
  - Budgeting
  - Capital planning
  - Product development
  - M&A due diligence

Action #9: Mature Evidence for Legal Defensibility

- Evidence is now:
  - Traceable
  - Time-bound
  - Custodian-assigned
- Supports:
  - Regulators
  - Insurers
  - Litigation defense

Phase 3: SCRMS-Native Operations (180–365 Days) (continued)

Action #10: Decide ISO’s Future Role

At this point organizations typically choose one:

- Maintain ISO only where contractually required.
- Scope ISO narrowly.
- Allow certification to lapse intentionally.
- Replace ISO with SCRMS-based conformity.

The decision is strategic, not forced.