Information Security Governance & Control Framework Guide

Strategic Architecture for Implementing Enterprise Security Operations

Document ID: ISC-FRM-00-PREVIEW
Effective Date: August 30, 2026
Version: 2.0 (Sample Edition)
Classification: Public Domain / Reference
Author: ISCSECURITY Architecture Team
Next Review: August 30, 2027

1. Purpose & Scope

This guide establishes the overarching governance architecture, risk taxonomy, and operational lifecycle required to maintain an enterprise information security management system (ISMS). It is designed as the **master reference document** that defines *what* must be controlled and *why*, while delegating the granular *how* to dedicated Standard Operating Procedures (SOPs).

Scope covers all personnel, third-party vendors, networked assets, cloud tenants, and data processing activities under the organization's direct or indirect control.

2. Governance & RACI Matrix

Clear accountability prevents overlap and omission. The following matrix defines responsibility for core framework activities:

Activity	CISO	SOC Lead	IT Manager	HR / Legal
Policy Development	Accountable	Consulted	Consulted	Informed
Risk Assessment	Accountable	Responsible	Consulted	Informed
Incident Declaration	Accountable	Responsible	Informed	Informed
Access Revocation	Approved	Informed	Responsible	Accountable
Vendor Risk Acceptance	Accountable	Consulted	Responsible	Approved

3. Information Risk Classification Model

All corporate data and systems must be classified according to the impact of unauthorized disclosure, alteration, or destruction.

Level	Criteria	Handling Requirements
Level 1 — Public	Approved marketing material; published press releases.	Standard integrity controls; no encryption required at rest.
Level 2 — Internal	Operational handbooks, org charts, internal memos.	Access control required; encryption in transit (TLS 1.2+).
Level 3 — Confidential	Customer PII, financial forecasts, audit findings.	Role-based access; AES-256 at rest; logging mandatory.
Level 4 — Restricted	Security architecture; incident forensics; cryptographic keys.	Need-to-know only; MFA mandatory; air-gapped backups.

4. The 14-Control Operational Pillar Map

This framework is executed through fourteen discrete operational playbooks. The matrix below maps each SOP to its parent NIST Cybersecurity Framework function and relevant ISO 27001:2022 Annex A controls.

Pillar / SOP	NIST CSF 2.0	ISO 27001:2022	Availability
Incident Response & Containment	Respond (RS)	A.5.24, A.5.25	PAID TEMPLATE
Phishing Investigation & Triage	Detect (DE)	A.5.7, A.5.23	PAID TEMPLATE
Ransomware Mitigation	Respond (RS)	A.5.29, A.8.1	PAID TEMPLATE
User Provisioning / De-provisioning	Protect (PR)	A.5.15, A.5.16, A.5.18	PAID TEMPLATE
Privileged Access Review	Protect (PR)	A.5.18	PAID TEMPLATE
MFA Enforcement	Protect (PR)	A.5.17	PAID TEMPLATE
Patch Management	Protect (PR)	A.8.8, A.8.9	PAID TEMPLATE
Vulnerability Assessment	Identify (ID)	A.5.7, A.8.8	PAID TEMPLATE
Asset Lifecycle & Disposal	Protect (PR)	A.5.09, A.8.1	PAID TEMPLATE
Data Backup & Recovery	Recover (RC)	A.5.29, A.8.1	PAID TEMPLATE
Vendor / Third-Party Risk	Govern (GV)	A.5.19, A.5.20	PAID TEMPLATE
Change Management Control	Protect (PR)	A.5.29, A.8.8	PAID TEMPLATE
Security Awareness & Phishing Simulation	Protect (PR)	A.6.3, A.6.4	PAID TEMPLATE
Acceptable Use Enforcement	Govern (GV)	A.5.11, A.6.3	PAID TEMPLATE

5. Operational Lifecycle Workflow

Security controls are not static artifacts. They follow a continuous cycle:

1. **Identify & Classify:** Map assets, classify data (per Section 3), and determine risk appetite.
2. **Implement Controls:** Deploy the technical and procedural controls defined in the relevant SOPs above.
3. **Monitor & Detect:** Aggregate telemetry, audit logs, and anomaly thresholds to identify deviations.
4. **Respond & Recover:** Execute incident response phase gates; restore services via backup protocols.
5. **Review & Improve:** Annual management review, access re-certification, and policy gap analysis.

6. Sample Extract: Incident Response Phase Gates

To demonstrate the depth of our operational playbooks, the following high-level phase gates are excerpted from the full *Incident Response and Containment SOP* (Pillar 1). This preview illustrates strategic decision trees; the complete template contains workstation isolation commands, forensic chain-of-custody templates, and stakeholder communication scripts.

Phase	Objective	Key Decision Gate
Preparation	Ensure tools, contacts, and legal retainers are active.	Is the IR war room activated and lead assigned?
Detection & Analysis	Validate alert legitimacy and determine scope.	Is the event a false positive, minor incident, or material breach?
Containment	Limit blast radius without destroying evidence.	Short-term (isolation) vs. long-term (segmentation) strategy?
Eradication	Remove threat actor presence and restore integrity.	Has the root cause (IOC / vulnerability) been neutralized?
Recovery	Return systems to production with enhanced monitoring.	Have restored systems passed integrity baselines?
Post-Incident	Document lessons learned and update controls.	Have all SOP gaps been logged for the quarterly review?

Note: The full SOP includes technical runbooks for Active Directory isolation, memory acquisition, and regulatory breach notification timelines.

7. Compliance Mapping Summary

This governance framework directly satisfies control objectives from the following audit architectures:

- **SOC 2 Type II:** Trust Services Criteria CC1.0 (Control Environment), CC6.1 (Access Control), CC7.2 (System Monitoring), and CC8.1 (Change Management).
- **ISO/IEC 27001:2022:** Clauses 4–10 (Context, Leadership, Planning, Support, Operation, Evaluation, Improvement) and Annex A.5 (Organizational Controls).
- **NIST CSF 2.0:** Govern (GV) and Identify (ID) functions, providing the foundational context for Protect, Detect, Respond, and Recover.

8. Document Control & Revision History

Version	Date	Author	Description of Changes
1.0	2025-03-15	ISCSECURITY Arch	Initial draft for internal stakeholder review.
2.0	2026-08-30	ISCSECURITY Arch	Public evaluation release; mapped to 14 operational SOP pillars.
