RIDGELINE CYBER DEFENCE

Cybersecurity Governance Suite

Complete cybersecurity governance documentation covering all 49 MS-ISAC priority subcategories across NIST CSF 2.0, ISO 27001:2022, and CIS Controls v8.

DOCUMENTS	FRAMEWORKS	FORMAT
78+	NIST CSF 2.0, ISO 27001, CIS v8	Word (.docx) + Excel (.xlsx)

PRODUCT PREVIEW

This document provides a preview of the product contents, structure, and sample documentation quality. Visit ridgelinecyber.com to purchase the full toolkit.

WHAT'S INCLUDED

The Cybersecurity Governance Suite contains the following documents, templates, and tools:

Tier 1 — Policies (18 Documents)

- POL-001 Information Security Policy
- POL-002 Acceptable Use Policy
- POL-003 Access Control Policy
- POL-004 Data Classification and Protection Policy
- POL-005 Incident Response Policy
- POL-006 Business Continuity and Disaster Recovery Policy
- POL-007 Risk Management Policy
- POL-008 Network Security Policy
- POL-009 Change Management Policy
- POL-010 Vulnerability Management Policy
- POL-011 Physical and Environmental Security Policy
- POL-012 Third-Party and Supply Chain Risk Policy
- POL-013 Cryptography and Key Management Policy
- POL-014 Security Awareness and Training Policy
- POL-015 Logging, Monitoring, and Auditing Policy
- POL-016 Secure Software Development Policy
- POL-017 Privacy and Data Protection Policy
- POL-018 Asset Management Policy

Tier 2 — Standards and Processes (22 Documents)

- STD-001 through STD-012: Technical standards covering password, encryption, hardening, patching, backup, network segmentation, logging, mobile device, cloud security, endpoint, data retention, and remote access
- PRC-001 through PRC-010: Operational processes covering risk assessment, incident response, change management, vulnerability management, access reviews, BCP/DR testing, security awareness delivery, third-party assessment, data classification, and audit/compliance review

Tier 3 — Procedures (18 Documents)

- PROC-001 through PROC-018: Step-by-step operational procedures covering account provisioning, malware response, backup/restore, firewall rule changes, security event triage, patch deployment, new user onboarding, data destruction, vulnerability scanning, incident evidence collection, system hardening, access review execution, security tool deployment, password reset, phishing response, log review, physical access management, and change implementation

Tier 4 — Forms and Templates (20 Documents)

- FRM-001 through FRM-020: Working Excel and Word tools including risk register, incident report form, change request form, access request form, BCP test report, vulnerability assessment report, third-party questionnaire, security exception request, asset inventory template, training record tracker, audit findings tracker, data classification worksheet, policy acknowledgement form, security metrics dashboard, DR test plan, evidence collection log, vendor risk scorecard, security budget template, compliance gap tracker, and board reporting template

SAMPLE DOCUMENT EXCERPT

Information Security Policy

Document ID: POL-001 | Version: 1.0 | Classification: Internal | Status: Template

1. Purpose

[Organisation Name] recognises that information is a critical business asset that must be appropriately protected against threats to its confidentiality, integrity, and availability. This policy establishes the strategic direction and governing principles for information security across the organisation, ensuring that information assets are protected commensurate with their value and associated risk exposure. This policy applies to all information assets owned, controlled, or processed by the organisation, regardless of form or format.

2. Scope

This policy applies to all employees, contractors, temporary staff, volunteers, and third parties who access, process, store, or transmit organisational information or use organisational information systems. It covers all information assets including electronic data, paper records, intellectual property, and information processing facilities across all locations, including remote working environments and cloud-based services.

3. Policy Statements

3.1 The organisation shall establish, implement, maintain, and continually improve an Information Security Management System (ISMS) aligned with recognised international standards and frameworks, including NIST CSF 2.0 and ISO/IEC 27001:2022. 3.2 Information security risk management shall be integrated into the organisation's enterprise risk management framework. Cybersecurity risks shall be identified, assessed, prioritised, and treated in accordance with the organisation's defined risk appetite and tolerance levels. 3.3 Information assets shall be classified according to their sensitivity and criticality, and protected with controls proportionate to their classification level throughout their lifecycle.

4. Roles and Responsibilities

4.1 The Board of Directors / Senior Leadership shall provide strategic direction and oversight for information security, approve this policy and the information security strategy, allocate adequate resources, and foster an organisational culture that prioritises cybersecurity risk management. 4.2 The Chief Information Security Officer (CISO) or equivalent shall be responsible for developing, implementing, and maintaining the information security programme, reporting on the state of information security to senior leadership, and ensuring alignment with applicable frameworks and regulatory requirements.

This is a preview excerpt. The full document continues with additional sections including detailed implementation requirements, roles and responsibilities, compliance measures, exceptions process, and review procedures.

FRAMEWORK CROSS-MAPPING EXAMPLE

Every document in the toolkit includes framework traceability. Below is an example of how our documentation maps to multiple compliance frameworks simultaneously.

NIST CSF 2.0	ISO 27001:2022	CIS Controls v8	RidgeLine Document
GV.PO-01	A.5.1	CIS 1.1	POL-001 Information Security Policy
GV.RR-02	A.5.2	CIS 1.2	POL-001 Roles and Responsibilities
PR.AA-05	A.5.15, A.8.2	CIS 5.1, 6.1	POL-003 Access Control Policy
PR.DS-01	A.8.24	CIS 3.6, 3.11	POL-004 Data Classification Policy
DE.CM-01	A.8.15, A.8.16	CIS 8.2, 8.5	POL-015 Logging and Monitoring Policy
RS.MA-01	A.5.24, A.5.26	CIS 17.1	POL-005 Incident Response Policy
ID.AM-01	A.5.9	CIS 1.1, 2.1	POL-018 Asset Management Policy
GV.RM-01	A.5.1, A.6.1	CIS 1.1	POL-007 Risk Management Policy

Ready to close your governance gaps?

The full Cybersecurity Governance Suite includes every document shown in this preview — plus all supporting standards, procedures, forms, templates, and cross-mapping workbooks.

Starting from $149

ridgelinecyber.com/cybersecurity-governance-suite/

contact@ridgelinecyber.com

14-day money-back guarantee | Instant download | Customise and deploy in days

This is a customisable template product only. It is not legal advice. Organisations should seek qualified professional advice for their specific circumstances and jurisdiction.