

Security Governance for Nonprofits

Practical and pragmatic assistance with security governance, backed by security professionals with real world experience — and a coaching approach that leaves capability behind.

The benefits

- Allocation of ownership of information security responsibilities across staff, volunteers and your board.
- Identification, communication and treatment of information security risks in language your board and funders understand.
- Development of documentation and implementation of process to pro-actively address deficiencies and satisfy auditors, insurers and grant conditions.
- Security governance and security operations process improvements that reduce risk, reduce cost and free funds for your mission.
- A maturity story you can show insurers and funders — measured against the Cloud Security Alliance's CCM Lite, an open standard your team can keep using.

Services can be provided via cybersecurity maturity coaching, long term secondment or small tactical advisory engagements, and leverage our model Information Security Management System. All deliverables are tailored to your organisation's mission and desired risk posture — enabling your organisation to gain traction on information security without re-inventing the wheel.

Typical security governance services

Cybersecurity Maturity Coaching

Our flagship service — we teach your team to fish. Hands-on coaching on Microsoft 365 security configuration including Intune (identity, device management, email security and data protection), and security governance using CSA CCM Lite: 91 foundational controls mapping to ISO, NIST and CIS, with implementation guidance so your team can self-improve quarter on quarter.

Security Posture Report

A gap analysis between relevant security standards (CSA CCM Lite, ISO 27001/27002), regulations (PCI-DSS for donation channels) and legislation (Privacy Act) and your current operations, followed by a risk assessment identifying where to focus effort for maximum risk reduction.

Virtual Chief Information Security Officer

We act on your behalf — with your support and approval — making informed management decisions about information security: setting strategy, performing assessments, developing documentation, advising project teams, conducting tenders and producing board reporting. Cost effective for nonprofits with high security obligations but no budget for a full-time hire.

Security Awareness Training

Engage and educate your board and senior stakeholders to build support for your security program; and induction and refresher training for staff and volunteers that raises awareness of security threats — especially the phishing and payment redirection fraud that targets charities.

Our Model Information Security Management System

Our model ISMS provides a ready frame of reference for security posture assessments and the ability to rapidly develop security documentation and implement security processes tailored to an organisation's size, mission, desired risk profile and allocated information security budget. In coaching engagements, your team learns to own and operate every layer.

Information Security Charter

Records board and senior management commitment to information security and sets the strategic direction for the security program.

Information Security Policy

Establishes the requirements for security standards through policy statements that set the desired risk profile for the organisation.

Information Security Standards

Captures security requirements (controls) in the form of standard statements along with implementation guidance.

Information Security Processes

Enables the design of procedures and assists in the implementation of the majority of security controls from applicable standards.

Information Security Procedures

Step by step work instructions for high risk activities — like staff and volunteer onboarding and offboarding — providing repeatable and reliable operation of key security controls.

Blueprints · Risk Management · Metrics · Compliance

Security patterns for upcoming projects; documents to identify and capture risk; metrics for measuring and reporting control effectiveness; and a regime testing key controls to provide assurance they operate effectively.

Information Security Management Reporting

A procedure and templates for reporting to your board and funders on information security holistically — risk profile and security posture, not just raw statistics.