

Security Governance Wisdom

Practical and pragmatic assistance with security governance, backed by security professionals with real world experience.

The benefits

- Allocation of ownership of information security responsibilities.
- Identification, communication and treatment of information security risks.
- Development of documentation and implementation of process to pro-actively address deficiencies and avoid internal and external audit issues.
- Security governance and security operations process improvements that reduce risk, reduce cost and enable new business initiatives.
- Benchmarking of your security function against other organisations in terms of functionality, capability and effectiveness.

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

Typical security governance services

Security Posture Report

A gap analysis between relevant security standards (ISO 27001/27002, the Australian Government Information Security Manual), regulations (PCI-DSS) and legislation (Privacy Act, Health Records Act) and your current operations, followed by a risk assessment identifying where to focus security effort for maximum risk reduction — with tactical and strategic recommendations you can act on.

Information Security Management System Development

Using our model ISMS template we rapidly develop security policy, standards, processes and procedures aligned with your organisation's risk appetite and the requirements of relevant legislation, regulation and security standards.

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, running security projects, conducting tenders, procuring technology and producing management reporting.

Security Awareness Training

Engage and educate senior business stakeholders to build support for your security program; tailored technical training on application and infrastructure security; and induction and refresher training that raises awareness of security threats and acceptable use obligations.

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, core operations, desired risk profile and allocated information security budget.

Information Security Charter

Records 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, 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 on information security holistically — risk profile and security posture, not just raw statistics.