FUJITSU

Security Documentation Suite

Clear, practical security documentation that supports governance, assurance and resilience

Engaging our security documentation services enables organisations to identify and address hidden risks early, reducing the likelihood of security incidents and regulatory non-compliance while providing clear, documented visibility of the environment and its security posture.

What we do

Our Advisory and Assurance team specialise in the design, delivery and uplift of security documentation tailored to technology environments and organisations of varying sizes, maturity and context. We establish clear and practical documentation that supports security governance, operational use and assurance activities.

The risks we help uncover

- Governance gaps.
- Configuration and security control drift.
- Undocumented or partially documented systems.
- Outdated or misaligned security standards.
- Inconsistent security practices.
- Limited assurance and audit defensibility.

Clear and consistent security governance

Stronger alignment between policy and practice

Improved risk visibility and confidence in controls

Audit and assurance readiness

We take a pragmatic and practical approach, working closely with stakeholders and subject matter experts to ensure governance intent is translated into clear, usable security artefacts that accurately reflect the operating environment.

Whether you require an end-to-end security documentation suite or targeted support uplifting security components of existing design documentation, we tailor our services to meet your needs.

Through the design, review and uplift of security documentation, we commonly uncover risks that are not always visible through technical assessments alone.

How structured documentation strengthens delivery and resilience

- Reduced reliance on individual knowledge holders.
- Faster and clearer onboarding for new staff, contractors and delivery partners.
- Improved consistency across teams, systems and environments.
- Increased confidence when responding to incident or regulatory reviews.

The importance of robust security documentation

Technology systems demand structured security documentation and governance to support resilience, accountability and informed decision-making. Where documentation has not been formally established or has not kept pace with organisational and technological change, security documentation can quickly fall behind the environment it is intended to govern.

Security documentation includes:

Security policies, standards and procedures, such as Information Security Policies, Event Logging and Monitoring Plans and Vulnerability and Patch Management standards to name a few.

Risk management frameworks and defined assessment and treatment processes that enable consistent identification and management of cyber risks.

Documentation aligned to regulatory standards and frameworks, such as ISO 27001, the Australian Information Security Manual (ISM), New Zealand ISM, and the Protective Security Policy Framework (PSPF).

Why choose us?

Proven delivery for government and private sector clients across Australian and New Zealand regulatory environments.

Practitioners with hands-on experience in cyber risk management, assurance and system governance.

Insight into how auditors and regulators assess security documentation and evidence.

If your security documentation no longer reflects your environment, or if documentation has yet to be formally established, contact us today.