Governance, Risk & Compliance Practice

Strategic information security that aligns to business objectives and creates enterprise wide resilience to current and emerging threats

"In an increasingly hyperconnected world, the impacts of our successes and mistakes are significantly magnified. Resilience of cyberspace could be strengthened by treating cyber security as a board-level issue..."
The World Risk Report, 2013 - The World Economic Forum

Today's businesses are supported by technology ecosystems that continue to evolve at a break neck speed. Online applications, 'big data', consumerism, mobile devices, and cloud computing are some of the paradigms shaping the way organisations use information to interact with their people, customers, and wider stakeholders.

To add to the complexity, organisations and IT executives are confronted with a workforce that places a high value on use of privately owned smart phones and tablets (the BYOD phenomenon) for business and personal purposes.

These trends are occurring in a global environment where security incidents across both public and private sectors have increased markedly.

In response, the Australian legislative and regulatory environment is becoming more rigorous, particularly in regard to personally identifiable data (PII) and other confidential information assets.

Certainly there is greater emphasis on executive level responsibilities in this area including a duty of care to maintain appropriate security of information under amendments to the Privacy Act. A renewed focus on the obligations of directors under aspects of the Corporations Act is expected for many.

Sense of Security's Governance, Risk and Compliance services are developed with the above environmental factors in mind.

Our approach combines best practice consulting methodology, risk based reporting, quality assurance principles underpinned by the extensive experience of our consultants. A typical engagement will focus on an organisation's compliance obligations, its operating context, information technology strategy, and the construct of its information assets.

The outcome is a client centric and professionally qualified deliverable that addresses your Governance, Risk and Compliance objective.

GOVERNANCE, RISK & COMPLIANCE

Information Security Management System
– ISO 27001/2 Development

Risk Management – ISO 31000 & 27005

Payment Card Industry Data
Security Standard (PCI DSS)

Australian Government Information
Security Standards (ISM, PSPF, NESAF)

Cloud Computing Security Governance

Mobility Security Governance

Secure Development Lifecycle

SECURITY STRATEGY & ARCHITECTURE

Information Security Strategy & Roadmap

Information Security Architecture

Information Security Policy
& Procedure Development

Cyber Threat
& Risk Assessment

Vulnerability Management

Data Classification
& Risk Treatment

SCADA Security Design & Review

Sense of Security®