Strategic Security Management Framework

Managing Security across the Enterprise
The Strategic Security Management Framework

Organisations need to invest the time and effort into developing an effective security management framework and to implement the technology around it!

An effective strategy drives all other practices and works to maintain those practices and it helps organisations react to new and emerging threats.
The Strategic Security Management Framework

Components of the SSMF

- Management and Governance
- Risk Assessment and Management
- Security Policies and Standards
- Compliance and Awareness
- Security Assurance
- Incident Management
- Performance and Metrics
- Legal and Regulatory Environment
Components of the SSMF
Management and Governance

Goal: To review, develop and maintain a Management and Governance Structure around IT Security and Risk Management that is in compliance with best practice standards and mandated business corporate governance legal and regulatory requirements.

- Develop an Security Organisational Structure
- Establish close ties to business executive
- Establish accountability and visibility for security at a executive level
- Define Roles, Responsibilities & Accountabilities
- Establish a Compliance assessment Program
Risk Assessment and Management

Goal: To review, develop and maintain a risk assessment and management program. To understand the enterprise environment ensuring that all potential risk exposures are assessed and actioned, encompassing all business entities and components.

- Environmental Scoping
- Risk Management and Assessment Methodologies and Processes
- Current State Analysis and Business Impact Assessments
- Identify and Classify Information Assets
- Identify and normalise Regulatory & Compliance requirements
Policies and Standards

Goal: To review, develop and maintain a set of relevant, and in-line with good to best practice, IT Security Policies, Standards, Baselines/Procedures and Processes (where applicable), that outline how Information Technology is deployed and used within an organisation. (Inc. requirements such as PCI DSS)

- Assess adequacy of Policies.
- Integrate Security Controls from Risk Assessments in Business Procedures and Policies.
- Look at International Standards such as ISO 27001, PCI DSS, I7799:2005 as baseline controls.
- Assess the socialisation procedures for policies and standards.
Compliance and Awareness

Goal: To review, develop and maintain a compliance and awareness culture within the organisation to ensure that policies and standards as defined in the previous section are complied with across the whole organisation.

- Develop a Security Awareness Program
- Develop an ongoing assurance program for assessment of compliance against policies and assessments.
- Assess independent assessment, training requirements.
Security Assurance

Goal: To review, develop and maintain a security assurance review program/roadmap that ensures that what the organisation is expecting in terms of compliance is what is actually happening. This work is based upon business criticality, potential risk exposure and reaction to environmental changes. (inc. mandated compliance eg; PCI DSS)

Define requirements for ongoing assessments and management for:

- Vulnerability Management
- Application & Network Intrusion Testing
- Source Code Inspection
- Architecture Reviews
- System Build Reviews
- Internal Network Testing
- VOIP Testing
- Wireless Testing
- New and Emerging Threats.
Incident Management

Goal: To review, develop and maintain an Incident Management Program and Processes that will provide the basis for quick response and action to realised threats that the organisation is facing.

- BCP Business Impact Assessments
- Current State Analysis
- Policy Reviews
- Business Continuity Planning
- Incident Response Policies and Procedures
- Identify and Implement a Rapid Response Team with independent specialists where required.
Performance and Metrics

Goal: To review, develop and maintain a system that will track the effectiveness of the IT Security and Risk Management strategy and each component of the SSMF

- Identify Security Metrics
- Develop a performance assessment program against security metrics.
Legal and Regulatory Environment

Goal: To identify the complete set of security requirements driven by the organisations regulatory and legal environment that must be incorporated into the SSMF

• Compliance Requirements Analysis and Identification
• Security requirement mapping
• Policy Gap Assessment (Compliance Requirements)
About Security-Assessment.com

Helping organisations to:

- Understand their state of security
- Understand their security regulatory and compliance obligations
- Align security to the business
- Identify system and process weaknesses
- Develop robust, business appropriate security plans and policies
- Improve the quality of processes, applications and system builds.
- Plan for and respond to incidents