Strategy and architecture: Information Strategy: Information security SCTY

Description

The selection, design, justification, implementation and operation of controls and management strategies to maintain the security, confidentiality, integrity, availability, accountability and relevant compliance of information systems with legislation, regulation and relevant standards.

Level 7

Directs the development, implementation, delivery and support of an enterprise information security strategy aligned to the strategic requirements of the business. Ensures compliance between business strategies and information security and leads the provision of information security resources expertise, guidance and systems necessary to execute strategic and operational plans across all of the organisation's information systems.

Level 6

Develops and communicates corporate information security policy, standards and guidelines. Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks. Leads the provision of authoritative advice and guidance on the requirements for security controls in collaboration with experts in other functions such as legal, technical support. Ensures architectural principles are applied during design to reduce risk and drives adoption and adherence to policy, standards and guidelines.

Level 5

Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security, and recommends appropriate control improvements. Contributes to development of information security policy, standards and guidelines.

Level 4

Explains the purpose of and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls. Performs security risk, vulnerability assessments, and business impact analysis for medium complexity information systems. Investigates suspected attacks and manages security incidents. Uses forensics where appropriate.

Level 3

Communicates information security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to vulnerability assessments. Applies and maintains specific security controls as required by organisational policy and local risk assessments. Investigates suspected attacks. Responds to security breaches in line with security policy and records the incidents and action taken.