# Information security SCTY

Defining and operating a framework of security controls and security management strategies.

|  |
| --- |
| **Guidance Notes:**The purpose of security controls and management strategies is to:* maintain the security, confidentiality, integrity, availability, accountability of information systems
* ensure information systems comply with legislation, regulation and relevant standards.

Activities may include, but are not limited to:* selecting, adopting and adapting security control frameworks
* designing, justifying and implementing security management strategies
* identifying risks with technical solution architectures
* ensuring security principles are applied during design and development to reduce risk.

Examples of types of security controls include, but are not limited to:* physical controls
* procedural or administrative controls
* technical or logical controls
* legal and regulatory or compliance controls.

These activities are typically performed in collaboration with specialists in other areas including, but not limited to, legal, technical infrastructure, audit, architecture, software engineering. |

## Level 2

Assists with information security tasks under routine supervision.
Supports the application of basic security controls.
Helps document and report security issues and risks.
Helps investigate suspected attacks and security breaches.

## Level 3

Applies and maintains specific security controls as required by organisational policy and local risk assessments.
Communicates security risks and issues to business managers and others. Performs basic risk assessments for small information systems.
Contributes to the identification of risks that arise from potential technical solution architectures. Suggests alternate solutions or countermeasures to mitigate risks. Defines secure systems configurations in compliance with intended architectures.
Supports investigation of suspected attacks and security breaches.

## Level 4

Provides guidance on the application and operation of elementary physical, procedural and technical security controls.
Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems.
Identifies risks that arise from potential technical solution architectures. Designs alternate solutions or countermeasures and ensures they mitigate identified risks.
Investigates suspected attacks and supports security incident management.

## Level 5

Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards.
Contributes to development of information security policy, standards and guidelines.
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.
Develops new architectures that mitigate the risks posed by new technologies and business practices.

## Level 6

Develops and communicates corporate information security policy, standards and guidelines.
Ensures architectural principles are applied during design to reduce risk. Drives adoption and adherence to policy, standards and guidelines.
Contributes to the development of organisational strategies that address information control requirements. Identifies and monitors environmental and market trends and proactively 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 subject matter experts.

## Level 7

Directs the development, implementation, delivery and support of an enterprise information security strategy aligned with the business strategy.
Ensures compliance between business strategies and information security.
Leads the provision of information security expertise, guidance and systems needed to execute strategic and operational plans.
Secures organisational resources to execute the information security strategy.