|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TSC Category** | Strategy Planning and Implementation | | | | | |
| **TSC Title** | Security Strategy | | | | | |
| **TSC Description** | Establish the organisation's security vision, strategy and initiatives to ensure adequate protection of assets. This involves the planning, implementation and review of enterprise-wide security controls which includes policies, processes, physical infrastructure, software and hardware functions to govern and preserve the privacy, security and confidentiality of the organisation's information and assets | | | | | |
| **TSC Proficiency Description** | **Level 1** | **Level 2** | **Level 3** | **Level 4** | **Level 5** | **Level 6** |
|  |  |  | **ICT-SNA-4021-1.1** | **ICT-SNA-5021-1.1** | **ICT-SNA-6021-1.1** |
|  |  |  | Assess security risks, threats and vulnerabilities, and recommend security initiatives to mitigate them | Establish security goals and objectives as well as policies and standards to guide information security and assurance in the current and future landscape | Create a security vision for the organisation and establish an overarching information security strategy and frameworks |
| **Knowledge** |  |  |  | * Security risks, threats and vulnerabilities * Linkage of business processes to security systems * Techniques and considerations in security programme design * Application of information security and assurance architectures * Existing internal and external security standards | * Goal setting and objectives of organisation security * Information security and assurance strategy * Best practices in information security policies * Best practices and emerging technologies in security control * Knowledge on the various security management benchmarks * Gap analysis in organisation security * Implications and impact of security gaps | * Vision and strategy development for organisational security * Key principles of information security and assurance * Industry standards, frameworks and best practice in information classification and permissions * Business impact projection and analysis * Industry best practices and benchmarks or standards in organisational security * Emerging security risks, threats and vulnerabilities |
| **Abilities** |  |  |  | * Identify security risks, threats and vulnerabilities relevant to organisation operations and systems. * Assess gaps in existing security controls and their potential business impact * Translate security objectives and assessment of gaps into specific security programmes or guidelines * Develop a detailed action plan for a security programme, making periodic updates with technological or regulatory changes * Deliver advice and guidance to facilitate adoption of information security and assurance architectures * Monitor the effectiveness of security initiatives, against internal and external standards | * Formulate security goals and objectives based on an integrated understanding of business priorities, the overarching security vision and strategy directions, and defined security management benchmarks * Establish standards and practices to protect the integrity, authenticity and confidentiality of information * Manage compliance with information security guidelines and classification or permission rules * Lead communication of security goals and objectives to the organisation * Review existing security controls against current and future costs / risks to the business * Develop strategies and plans to resolve security gaps * Drive organisation-wide security initiatives in line with internal and external standards | * Establish a vision and overarching strategy for the security of the organisation * Direct an organisation-wide strategic information security framework * Determine data protection policies for information classification and permissions in line with the business and security strategy * Define the security management benchmarks to evaluate formulated security goals and objectives * Allocate resources for security initiatives based on the relative impact and importance to the business * Review security initiatives to ensure alignment with internal and external standards * Anticipate potential security risks, threats and vulnerabilities faced to ensure the organisation's security controls are future-ready |
| **Range of Application** |  | | | | | |