|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TSC Category** | Risk Management, Governance and Regulatory Compliance | | | | | |
| **TSC Title** | Security Governance | | | | | |
| **TSC Description** | Develop and disseminate corporate security policies, frameworks and guidelines to ensure that day-to-day business operations guard or are well protected against risks, threats and vulnerabilities | | | | | |
| **TSC Proficiency Description** | **Level 1** | **Level 2** | **Level 3** | **Level 4** | **Level 5** | **Level 6** |
|  |  |  | **ICT-SNA-4020-1.1** | **ICT-SNA-5020-1.1** | **ICT-SNA-6020-1.1** |
|  |  |  | Proactively identify security risks in business operations and implement security guidelines and protocols, in line with corporate security policies | Evaluate security risks and establish corporate security policies and frameworks to guard against them | Anticipate potential security threats and emerging trends in security management, establishing targets for the organisation's security policies and systems |
| **Knowledge** |  |  |  | * Organisation security operational procedures * Implementation process and considerations for security policies and protocols * Types of security controls and implementation procedures * Techniques for assessment of processes against security standards | * Security gap analysis * Security threats and system vulnerabilities * Critical elements of corporate security policies * Security frameworks * Key messages to drive in communication of security standards | * Potential internal and external threats to organisational security * Emerging trends and developments in security management and practices * Industry standards and best practices for organisational security * Impact of changes in security protocols on the organisation * Industry best practices and benchmarks for security frameworks |
| **Abilities** |  |  |  | * Assess adherence of applications and infrastructure components to security standards and baselines * Identify lapses in organisational security standards or issues that may endanger information security and integrity * Develop specific action plans for different business units, based on corporate security policies, standards and guidelines * Evaluate technologies and tools that can address security gaps and facilitate alignment with security policies * Introduce security controls in line with corporate security policies and frameworks * Roll out security guidelines and protocols, ensuring understanding and compliance * Review adequacy of information security controls * Highlight areas for improvement and propose solutions or revisions to security guidelines | * Identify existing security risks, threats and vulnerabilities and analyse gaps in current organisational security policies * Develop corporate security policies based on organisation's direction, to ensure business operations are well protected * Recommend improvements, updates or modifications to current security policies and practices, to address potential security gaps * Introduce suitable technologies, processes and tools to monitor, guide and maximise compliance with security policies * Drive communication of corporate security policies and implementation of security protocols * Establish internal processes to regularly review adequacy of information systems' security controls against set benchmarks | * Set direction for the organisation's corporate security policies, frameworks and protocols, in line with business requirements and the external environment * Endorse proposals for updates or enhancements to corporate security policies * Establish benchmarks and targets for information systems operations and processes to be regularly reviewed against |
| **Range of Application** |  | | | | | |