TSC Category	Power Systems Monitoring and Control					
TSC Title	Operational Technology Security Audit					
TSC Description	Manage audit and penetration testing on operational technology security systems					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
				<Insert TSC Code>	**<Insert TSC Code>**	**<Insert TSC Code>**
				Perform audits on operational technology security systems through penetration testing and vulnerability assessments	Lead audits, penetration testing and vulnerability assessments, and identify areas of non-compliance based on audit findings	Approve audit results and recommend measures to strengthen the operational technology security systems
Knowledge				• Application and usage of basic vulnerability assessment tools and tests • General process and technical requirements of penetration testing • Internal and external operational security standards • Methodologies and tools for the conduct of audit activities • Interpretation and analysis of audit results • International Electrotechnical Commission (IEC) 62443 • International Organisation for Standardisation (ISO) 27001/19 • Relevant regulations, industry standards, codes of practice and safety procedures	• Organisational objectives of vulnerability assessment and penetration testing • Key components and methodologies in the design of operational security testing activities • Elements and considerations in development of compliance processes • Evolving statutory and regulatory standards Application and relevance of external standards to organisation's context • Process gap analysis for business and operational technology (OT) operations • Relevant regulations, industry standards, codes of practice and safety procedures	• Design guidelines and best practices for threat modelling, vulnerability assessment, penetration tests and review • Process and key considerations in audit and compliance strategy development • Emerging trends, approaches and industry best practices in internal audit and compliance • Impact of business priorities and external regulations on audit strategy • Root cause evaluation of non-compliance in business and operational technology (OT) processes • Relevant regulations, industry standards, codes of practice and safety procedures
Abilities				• Perform technical coordination of	• Design security testing plan and evaluation	• Establish organisation guidelines and

				vulnerability assessments and penetration testing according to test plan templates • Execute vulnerability scans on smaller systems, using basic vulnerability assessment tools and tests • Document the results of security assessments and tests, according to test plan guidelines • Identify security lapses in the system or security mechanisms, based on issues documented from vulnerability scan results • Record evidence of controls which are inadequate or not duly enforced • Conduct audit activities in line with the organisation's compliance processes and guidelines, using appropriate methodologies and tools • Analyse audit results and highlight identified process gaps or key instances of noncompliance • Propose improvements to existing compliance processes and measures to address major risks • Implement changes in the performance of audits in alignment with changes in internal compliance standards or	criteria for vulnerability assessments and penetration testing activities • Manage implementation of vulnerability assessments and penetration testing activities, in line with organisation-wide strategy • Develop compliance processes in accordance with organisation's strategy and internal and external guidelines • Evaluate audit results to identify reasons for gaps or non-compliance in business and OT operations • Recommend enhancements to compliance processes to strengthen the organisation's internal controls	methodologies for the design and conduct of vulnerability assessments and penetration testing activities • Formulate implementation strategies for vulnerability and penetration testing activities to ensure organisation-wide consistent of information security plans • Authorise penetration testing activities on organisation's systems, in line with business priorities and security requirements • Synthesise key organisational implications from vulnerability assessment and penetration testing reports • Evaluate future readiness of the organisation's security posture in light of organisation's mission and the evolving technological environment • Establish audit and compliance strategy and objectives for the organisation, considering emerging trends, approaches and industry best practices • Oversee alignment of audit and compliance strategy with internal business requirements

				external regulatory guidelines		and priorities as well as external regulations and standards • Evaluate root causes and potential organisational impact or risks of non-compliance to prioritise the areas that require further enhancement • Endorse enhancements to critical compliance processes, to improve the robustness of organisation's internal controls
Range of Application				Range of application includes, but is not limited to: • Power Generation • Distributed Power Generation • Power Transmission and Distribution Network Systems used in monitoring and control of the power system, including but not limited to: energy management systems, information technology (IT) and operational technology (OT) systems, substation remote control unit (RCU) systems, flexible AC transmission systems (FACTS), and supervisory control and data acquisition (SCADA) systems		