TSC Category	Power Systems Monitoring and Control					
TSC Title	Cyber Incident Management					
TSC Description	Detect and report cyber incidents, identify affected systems and user groups, trigger alerts and announcements to relevant stakeholders, and ensure efficient resolution of situations					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
			<Insert TSC Code>	**<Insert TSC Code>**	**<Insert TSC Code>**	**<Insert TSC Code>**
			Provide real-time incident and status reporting, and identify affected systems and user groups	Troubleshoot cyber incidents, escalate alerts to relevant stakeholders, and identify root causes and implications of incidents	Implement cyber incident management procedures, synthesise incident-related analysis to resolve incidents, and establish mitigating and preventive solutions	Guide cyber incident management strategies for the remediation, resolution, communication and post-mortem of cyber incidents
Knowledge			• Incident detection and reporting protocols • Types of security incidents • Categorisation guidelines for incidents • Impact of incidents on systems and users	• Prioritisation criteria for incidents • Tools and processes used to remedy incidents • Root cause analysis procedures • Security implications of incidents	• Mechanics of incident alert triggers • Incident remediation solutions and strategies • Incident mitigation strategies	• Industry standards and best practices in incident management • Key components of an incident management playbook • Criteria and requirements of an incident response team • Cyber incident mitigation strategies • Key stakeholder groups • Post-mortem processes • Political and national sensitivities • Potential impact of incidents to the organisation and stakeholders

Abilities			• Maintain a tracker or log of incidents to provide real-time status reporting on affected systems • Report incidents, in line with incident management protocols • Gather relevant information about incidents • Categorise the importance of incidents based on established guidelines • Identify the systems and user groups affected by the incident based on information gathered • Assist in mitigation of repeat incidents as directed • Document the modifications made to troubleshoot and resolve problems or incidents in the system	• Review categorisation of an incident, and determine its priority and need for escalation • Escalate alerts to relevant stakeholder groups upon the occurrence of incidents • Perform first responder troubleshooting on cyber-related or security incidents, by following pre-determined procedures • Analyse incident reports, log files and affected systems to identify threats and root causes of incidents • Perform incident triage to assess severity of incidents and security implications • Implement approved processes or technologies to mitigate future incidents	• Develop mechanisms or threat signatures that trigger incident alerts to relevant parties and systems • Integrate cyber-related information, alerts and analysis from detection system logs to develop a holistic view of incidents • Distil key insights and impact from analyses of incidents • Manage the containment of cyber incidents within the organisation • Lead recovery of contained security incidents • Establish mitigation and prevention processes and policies • Drive implementation of mitigation processes and policies	• Establish incident management procedures for the detection, reporting and handling of incidents • Develop a playbook for cyber incident management • Lead an incident response team • Lead the remediation and resolution of cyber incidents at the organisational level • Resolve large-scale, unpredictable incidents • Make key decisions on when and how to communicate incidents to different critical stakeholders • Direct post-mortem activities following critical incidents • Develop organisation-wide cyber incident mitigation strategies • Lead critical communications to the public, authorities, internal and external stakeholders
Range of Application			Range of application includes, but is not limited to: • Power Generation • Distributed Power Generation • Power Transmission and Distribution Network			