POWER ENGINEERING COMPETENCY FRAMEWORK FOR POWER ENGINEERING PROFESSIONALS IN PUBLIC SERVICE
TECHNICAL SKILLS AND COMPETENCIES (TSC) REFERENCE DOCUMENT

TSC Category	Power Systems Monitoring and Control					
TSC Title	Cyber Risk Detection and Monitoring					
TSC Description	Manage the detection and monitoring of cyber risks to ensure that power systems are safe from cyber threats and information security issues					
TSC Proficiency Description	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**	**Level 6**
		<Insert TSC Code>	**<Insert TSC Code>**	**<Insert TSC Code>**		
		Support the detection and monitoring of cyber risks and information security issues in power systems	Assess cyber risks and information security issues in power systems	Review, report and escalate cyber risks and information security issues in power systems		
Knowledge		• Methods and tools for monitoring activities, systems and mechanisms • Intrusion detection techniques, software, and their functions • Types of security risks and intrusions • Security protocols, standards and data encryption • Indicators of cyber attacks • Attack patterns and threat vectors • Techniques, methods and technologies in threat data collection	• Range of intrusion detection and monitoring technologies • Applied principles and tools of information security • Techniques for analysis and integration of threat data • Relevant data sources of threat intelligence in the form of firewall logs, intrusion detection system logs, open source internet searches, honeypots • Types and features of exploits and malware	• Mechanisms for threat detection and monitoring • Advanced statistical and trend analysis techniques • Emerging trends and developments in cyber security • Impact analysis of cyber threats • Range of possible tactics, techniques and procedures used for security attacks • Key components and objectives of intelligence products and mission reports		
Abilities		• Install security applications and appliances for detecting intrusions and guarding against cyber attacks and information security breaches • Monitor access control mechanisms, activities and operating systems	• Identify resources and technologies required for intrusion detection according to technical and cost guidelines • Implement intrusion detection and analysis based on key objectives and stakeholders' requirements	• Develop strategies for risk monitoring and tracking efforts across systems • Perform advanced trend, pattern and statistical analysis to project future technical cyber threat scenarios • Synthesise multiple information sources and		

		• Interpret information from logs and scanners to detect threats and intrusion attempts • Apply detection technologies, checks and techniques to identify anomalous activity and patterns • Recognise indicators of attacks during the detection process • Follow-up with relevant parties on any security risks or intrusions detected • Use technologies, methods and tradecraft to retrieve and organize threat data or information	• Analyse collected information to identify vulnerabilities and potential for exploitation • Review multiple sources of data and intelligence feeds • Conduct intelligence analysis of cyber activities to identify entities of interest, potential methods, motives, and capabilities • Present information to place cyber-attacks in context • Integrate information to support the creation of internal cyber threat intelligence products	analysis reports into a holistic view of potential risk • Draw insights about the potential impact of estimated cyber threat scenarios • Develop mission reports and threat intelligence products that leverage to present analysis of threat data to key stakeholders • Lead comprehensive evaluation of the capabilities and activities of cyber criminals, foreign intelligence entities or perpetrators • Conduct in-depth research into cyber security issues of industry-wide or nationwide significance • Document findings to help initialise or support law enforcement and counterintelligence investigations or activities		
Range of Application		Range of application includes, but is not limited to: • Power Generation • Distributed Power Generation • Power Transmission and Distribution Network				