Position Description (PD)	
Role	Cyber Security Manager
Branch	Corporate Group
Team	Digital Technologies (DT)
Level	Executive Level 1
Role context	**About the Team** The DT team ensures that all aspects of DT can support the continuity of current business operations while delivering new capabilities to support evolving business needs. The team leads the innovative application of technology to meet the Productivity Commission's (PC's) strategic objectives while keeping core systems and information available, accessible, and secure. The Cyber Security Manager is a key leadership role responsible for overseeing and advancing the PC's cybersecurity strategies, policies, and programs. The role will manage the security infrastructure and ensure the protection of the PC's information assets against cyber threats.
Reports to	Director, Digital Technologies
Direct reports	0-1
Responsibilities	Key responsibilities of the role include: • Implementation of the actions identified during a recent internal audit, to uplift the PC's compliance with the Essential 8. ○ As part of this, demonstrate actions to members of the DT team, to provide on-the-job coaching and knowledge transfer, thereby eliminating key person risk. • Develop and implement a cybersecurity strategy aligned with PC goals and relevant government frameworks. • Provide expert advice to management and staff on cyber security risks and strategies, including the preparation of regular reports and training. • Conduct regular risk assessments and vulnerability analyses to identify and mitigate potential security threats. • Coordinate with internal and external auditors to manage security assessments and audits using ASD Blueprint for 365 and Essential 8 strategies. • Lead the response to cybersecurity incidents, including investigation, containment, eradication, and recovery. • Develop and maintain incident response plans, ensuring preparedness for potential cyber threats.

	• Implement and oversee continuous monitoring of security systems and networks. • Develop and maintain key performance indicators (KPIs) and metrics to measure the effectiveness of cybersecurity programs. • Other duties as required.
Selection Criteria	**Professional expertise:** • Significant experience in a similar role/industry, and tertiary qualifications in Cyber Security or relevant industry certifications / experience (CISM, CISSP, CISA) • Proven success in technology Service Delivery and/or Service Operations roles • Service desk management experience covering issue, incident and problem management utilising modern service management platforms. • Demonstrated project management skills, including the ability to identify problems and negotiate satisfactory outcomes. • Strong Microsoft 365 experience in security areas (365 Defender) and Azure portal services • Experience with implementing and auditing ASD strategies to mitigate cyber security incidents (including Essential eight maturity model) and the Information Security Model (ISM), and/or Security Framework (ISO27001/NIST) with modern platforms and technology. • Exceptional troubleshooting skills. **Effective Engagement:** • Proven ability to engage effectively with managers and team members from a range of backgrounds. • Written communication (all formats) contains accurate information and is clear, concise, well-structured, and uses suitable language. • Interacts confidently and credibly with colleagues and key stakeholders in a variety of contexts. • Maintains cooperative and positive relationships with colleagues and key stakeholders. • Builds professional networks to obtain and share information. **Personal Productivity and Growth:** • Works under limited direction and at times independently and takes responsibility for planning and progressing work and delivering agreed outcomes. • Effectively manages competing priorities. • Ability to work systems and procedures and works to improve these. • Able to use all technology/tools relevant to area of work.