Job Description – Cyber Security Testing Lead

Department	Operational Delivery Team, Information Security
Grade	13
Reporting to	Information Security GRC Manager
Direct reports (yes or no)	No
WTW Code	

Job Purpose

As Cyber Security Test Lead, you will be responsible for leading and managing all security testing activities across the organisation.

You will develop and implement a comprehensive security testing strategy, oversee penetration testing and vulnerability assessments, and ensure that security findings are managed and remediated effectively. You will provide technical direction, collaborate with cross-functional teams, and mentor team members to foster their professional growth and technical skills. You will also act as the primary point of contact between MIB and third parties who provide testing capability.

Your work will help ensure that MIB systems and applications remain secure and resilient against evolving threats.

Key accountabilities

Security Testing Leadership

- Lead and manage security testing activities, including (but not limited to) network, application, cloud, and internal security testing.
- Develop and implement a comprehensive security testing strategy and roadmap ensuring full coverage of the MIB estate.
- Provide technical guidance and support on complex security vulnerabilities and remediation efforts.
- Mentor and manage other members in the information security team involved in testing, supporting their professional development.

Key accountabilities

Testing Vulnerability Management

- Manage security findings from penetration tests, vulnerability scans, and internal security assessments, working with development teams to ensure timely remediation.
- Provide technical guidance and analysis of complex vulnerabilities as well as proposed remediation efforts.
- Ensure reliable validation of remediation actions.

Collaboration and Integration of Testing

- Collaborate with development, product, infrastructure, change and project teams to integrate security testing into the Secure Software Development Life Cycle (SSDLC).
- Prepare and present detailed reporting on security testing findings and the overall security posture to both technical and non-technical stakeholders.

Business Continuity and Continual Improvement

- Assist with business continuity testing, ensuring security controls and processes support organisational resilience.
- Stay up to date with the latest security threats, trends, and testing methodologies.
- Foster a culture of continuous improvement within the security testing team.

Role requirements

Essential

- Minimum of 5 years' experience in cyber security, with at least 2 years in a lead or senior role.
- Proven experience in managing and conducting penetration tests, vulnerability assessments, internal security testing, and security audits.
- In-depth knowledge of security testing tools such as Burp Suite, Nmap, Metasploit, and Kali Linux.
- Strong understanding of common web application vulnerabilities (OWASP Top 10) and network protocols.
- Excellent communication and leadership skills, with the ability to articulate complex security concepts to diverse audiences.
- Relevant certifications such as OSCP, CEH, or CISSP.

Role requirements

Desirable

- Experience with cloud security testing (AWS, Azure, GCP).
- Familiarity with DevSecOps principles and practices.
- Scripting or programming experience in Python, Ruby, or similar languages.
- Experience with threat modelling.
- Experience assisting with business continuity testing and planning.