A black and white logo

Description automatically generated with low confidence

|  |  |
| --- | --- |
| Role Title | Principal Cyber Security Consultant |
| Function & Dept. | Consultancy, Cyber |
| Career Growth Level | Contributing & Developing (D) |
| CGP Descriptor | Qualified specialists, recognised for their expertise, serving as pivotal contributors in various domains. These specialists play a vital role in influencing and shaping new business strategies, policies, practices, and content, catering to both external and internal customers. Their responsibilities may encompass problem-solving and the development and execution of purpose-driven solutions, often of a complex nature, to meet the specific needs of both external and internal customers |
| Team | Consultancy |
| Reports to | Cyber Operations Director |
| Role Purpose | The security landscape is changing which in turn is bringing new challenges and opportunities. The ability to support customers directly or through our services is critical to the ongoing success and reputation of the SCC business as a Managed Security Service Provider (MSSP).    Focussed on Cyber Security Advisory and GRC (Governance, Risk, and Compliance) the role holder will be responsible for managing and executing consultancy activities. The role will cover information security advisory and compliance across privacy regulation, and cybersecurity, including but not limited to, ISO27001, NIST, and CAF.    The Principal Cyber Security Consultant will be the subject matter expert leading project teams and liaising with other personnel to achieve customer requirements.    The successful candidate will demonstrate a passion not only for technology and technical solutions but also for people and relationships, building these both internally and externally to the organisation.    Continually looking for opportunities to evangelise on behalf of SCC to grow our reputation and increase our customer base. |
|  |  |
| Key Responsibilities | |
| 1. Lead with a consultative approach engaging with customers and/or internal teams to advise of the best solution and work very closely with our customers to build strong long-term relationships, always seeking to become a ‘trusted advisor’. 2. Define and implement the consultancy framework (focussed on GRC) to be adopted within SCC to meet the needs of our customers. 3. Develop client policies and procedures that comply with corporate and regulatory standards. 4. Staying up to date with relevant laws, regulations, and industry standards affecting customers and adapting our service offerings to be current. 5. Provide educational sessions to our sales teams on compliance requirements, risk management, and governance principles and how our services can help their customers. 6. Have or build a significant web presence utilising tools such as LinkedIn and Vendor events to grow the reputation and visibility of SCC. 7. Work collaboratively across SCC to further define our product set, enable go-to-market Cyber Security Advisory and GRC services through the design and implementation of service collateral for sales and delivery teams as required. 8. Providing guidance to clients on technical and operational security measures designed to help defend against cyber threats. 9. Work with the delivery and pre-sales teams to ensure technical sign-off of operational documentation and suggesting improvements as applicable. 10. Act as mentor and provide support to colleagues across the technical teams. 11. Supply technical and strategic input for ongoing development of portfolio and to bids, solutions, and RFP documents. 12. Input to the architecture direction for SCC Cyber ensuring solutions will meet client and operational deliverables. 13. Engage with the wider SCC sales teams to make them fully aware of our capabilities and expand our pipeline. 14. Identify skills gaps and define resource requirements as necessary to build capability and resilience to deliver cybersecurity advisory and GRC service offerings. | |
|  |  |
| Person Specification | |
| 1. Open minded approach to any challenge with a determination to succeed and the ability to listen, identify and accurately playback requirements to various stakeholders. 2. Solid grasp of information security requirements and capabilities across different industries. 3. Ability to guide engineering teams through the deployment where required; ability to write and review reports, procedures, and standards. 4. Familiarity and demonstratable experience with Cyber Security Standards of Regulatory Frameworks such as NIST, NCSC CAF, NIS, ISO, and PCI. 5. Awareness of working with Detect and Respond Security technologies such as SIEM, EDR, MDR, and XDR. 6. Demonstrable understanding of technical and Information Security configuration and controls across multiple technologies such as Cloud, Firewalls, Anti-Virus, Encryption, IDS/IPS, RAS, MFA (Multi Factor Authentication), MS Directory Services, Exchange, VMWare, Citrix/VDI, Networking, database and storage technologies. 7. Ability to guide engineering teams through the deployment where required; ability to write and review reports, procedures, and standards. 8. Awareness of common exploits and vulnerabilities and how these may be prevented. 9. To have already achieved SC (Security Clearance) or willingness to undergo the process for SC Clearance. 10. Ideally hold or be working towards recognised Information Security qualifications (e.g., CISSP (Certified Information Systems Security Professional), CISM, ISO 27001 Lead Implementer, CISSP ISSAP). | |

|  |  |  |
| --- | --- | --- |
| Key  Competencies |  | Level |
| 1. | Stakeholder Relationship Management | Level 2 |
| 2 | Planning and Organising | Level 2 |
| 3. | Presentation Skills | Level 2 |
| 4. | Business Acumen | Level 1 |
| 5. | Communication skills | Level 2 |
| 6. | Continuous Improvement | Level 2 |

|  |  |  |
| --- | --- | --- |
| Value Behaviours |  | Level |
| 1. | Responsibility | Level 2 |
| 2. | Passion | Level 2 |
| 3. | Customer First | Level 2 |
| 4. | Agility | Level 2 |
| 5. | Family | Level 2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Description | Approved by | Date |
| 1.0 | November 2023 | Original | HR | November 2023 |
| 1.1 | September 2025 | Update |  |  |