A black and white logo

Description automatically generated with low confidence

|  |  |
| --- | --- |
| Role Title | Principal Cyber Security Consultant |
| Function & Dept. | Consultancy, Cyber |
| Career Growth Level | Collaborating & providing Technical Knowledge (E) |
| CGP Descriptor | Specialist team members with experience of specific fields, may have some involvement in amending and constructing processes to criteria. Technically or Operationally knowledgeable in a defined field or, may have responsibility for key customer engagement activity |
| Team | Consultancy |
| Reports to | Cyber Operations Director |
| Role Purpose | Our portfolio of cyber security products and services continue to grow at pace. SCC Cyber are pleased to present the opportunity for an experienced security risk professional to join our talented team enhancing our ability to meet increasing customer demand and maintain market leading delivery capabilities.    Focussed on GRC (Governance, Risk, and Compliance), the role holder will be responsible for delivery of consulting services in support of the wider SCC Cyber team. The role will deliver core information security governance, risk and compliance capabilities into our customers ensuring they are supported in their requirements to meet or align with key cyber security standards including but not limited to, ISO27001, NIST, and CAF.    The Senior Cyber Security Consultant will be a subject matter expert working independently or as part of a delivery team where necessary to achieve customer requirements.    The successful candidate will demonstrate a passion not only for technology and security but also for people, building strong internal relationships across SCC and within our customer base.    They will support our growth through collaboration and engagement with key stakeholders to raise and promote awareness of SCC Cyber and its capabilities. |
|  |  |
| Key Responsibilities | |
| 1. Engage with customers to deliver exceptional consulting services and support the growth of GRC service offerings. 2. Act as a subject matter expert to advise upon and implement against key security standards and frameworks in support of customer requirements. 3. Develop client policies and procedures that comply with corporate and regulatory standards. 4. Maintain current knowledge relating to relevant security legislation, regulations, and industry standards that may affect SCC customers. 5. Support the Principal Cyber Security Consultant in cross-business engagement and sales enablement activities to promote security consulting services. 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 in support of the Principal Cyber Security Consultant in helping 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. Provide guidance to existing and potential customers on how the effective use technical and operational security measures can help reduce security risk within applicable security frameworks. | |
|  |  |
| Person Specification | |
| 1. Experience working either as a Consultant for an MSSP or within an information security risk management and governance role as a permanent member of a security team. 2. Exceptional verbal and written communication skills to ensure the highest standard of presentation and deliverables for our customers and across the wider SCC. 3. Verifiable and demonstrable expertise in information security requirements and capabilities across different industries and sizes of organisation. 4. Verifiable and demonstratable experience with security standards and frameworks such as but not limited to NIST, ISO 27000-series, ISO 22301, CSA CCM, CIS and NCSC CAF. 5. Awareness of technical security solutions such as SIEM, EDR, MDR, and XDR and their purpose within the context of an organisation’s security programme. 6. Ability to work closely with engineering teams to define requirements and processes associated with the effective use of technology solutions within our customer base. 7. Familiarity with the Microsoft security stack and other market-leading vendor offerings that support the effective mitigation of security risk is desirable. 8. To have already achieved SC (Security Clearance) or willingness to undergo the process for SC Clearance. 9. Holding any of the following recognised Information Security qualifications is advantageous:    1. CGRC    2. CISM    3. CISA    4. CRISC    5. ISO 27001 Lead Implementer / Lead Auditor    6. ISO 22301Lead Implementer / Lead Auditor | |

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

|  |  |  |
| --- | --- | --- |
| 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 |  |  |