

|  |  |
| --- | --- |
| Job Title | **Cyber Security GRC Principal** |
| Grade | A |
| Function | **Technology – IT Security and Service Management** |
| Job Purpose | 1. As a member of the Cyber Security team, this role will be accountable to the Information and Cyber Security Manager. 2. The Cyber Security GRC Team plays a crucial role in enabling good security practices by providing security policies, guidance, and education. They understand cyber security risks across the commission and provide assurance to the departmental Senior Information Risk Owner, and other senior stakeholders that these risks are effectively managed in the delivery of CQC objectives. 3. The role of the Principal involves leading a small team of risk and security professionals to deliver security risk and assurance activities across the CQC. This includes scoping and leading the programme of cyber security assurance, and measuring confidence levels that the security features, practices, procedures, and architecture of our network and information systems enforce CQC Information Security Policy. 4. The Principal is responsible for applying their understanding of information security and the organisational context to provide insight into the security implications of proposed business and technical changes, leading the new Secure by Design approach and acting as a trusted advisor in communicating these effectively to technical and non-technical stakeholders. |
| Accountabilities and Responsibilities | 1. Own the Information Security Assurance framework and programme. 2. Design and perform themed reviews to provide assurance of information security controls effectiveness. 3. Responsible for establishing and implementing the information security and technology risk management programme identifying any issues or risks with and ensuring remediation to within defined appetite 4. Identify, engage and manage 3rd party organisations to ensure appropriate security assurance activities are conducted to ensure the rigour of our assets 5. Lead on Secure by Design activities to ensure business and technical changes meet security requirements 6. Embed and continually mature the CQC Secure and Privacy by Design approach across the organisation 7. Own the Security culture, education and awareness programme 8. Liaise with other bodies to contribute to the maturing of cyber security practices across the Health and Social care industry 9. Role models inclusive behaviours in everyday interactions. 10. Promotes a culture of respect and fairness and understands personal responsibilities around delivering against CQC diversity and inclusion strategy. 11. Demonstrate competence and supports others to achieve behavioural excellence through our Success Profiles (**insert link**) ensuring yourself and those you work with are the best that they can be. 12. Role models and supports others to instil our values into everything that we do. |
| Skills and experience | Role Specific   1. Experience of working at a senior-level in a specialist area of Information Security 2. Experience of authoring governance documentation (standards, policies, reporting, proposals, analysis) 3. Understanding of common security standards, frameworks and regulations relating to the health industry environment (Data Security and Protection Toolkit (DSPT), ISO2700x (International standard for information security management), Centre for Internet Security (CIS), GDPR, Cyber Assessment Framework (CAF), MITRE (A framework for cyber adversary behaviour)) 4. Experience of delivering culture, training and awareness programmes 5. Strong knowledge of Security controls across Microsoft based technologies, Endpoints, IdAM, Networks, Applications, Email and Cloud 6. Experience of working with Senior stakeholder to champion the security agenda   General   1. Excellent interpersonal, communication, and presentation skills, including formal report writing experience 2. Knowledge and experience of utilising different media to communicate, educate and assess security issues, messages and training across a varied audience. 3. Willingness to learn and keep abreast of the ever-changing security landscape including trends and technologies and market issues and dynamics. 4. Great problem solving and organisational skills 5. Ability to lead and influence others in a calm manner when under pressure   Qualifications   1. Any of CISSP. CISM, CRISC, CISA (not essential, but desired) |
| Values & Behaviours  **Excellence**  In my work for CQC:   * I set high standards for myself and others, and take accountability for results * I am ambitious to improve and innovate * I encourage improvement through continuous learning, * I make best use of people’s time, and recognise the valuable contribution of others   **Caring**  In my work for CQC:   * I am committed to making a positive difference to people’s lives * I treat everyone with dignity and respect * I am thoughtful and listen to others * I actively support the well-being of others   **Integrity**  In my work for CQC:   * I will do the right thing * I ensure my actions reflect my words * I am fair and open to challenge and have the courage to challenge others * I positively contribute to building trust with the public, colleagues and partners   **Teamwork**  In my work for CQC:   * I provide high support and high challenge for my colleagues * I understand the impact my work has on others and how their work affects me * I recognise that we can’t do this alone * I am adaptable to the changing needs of others | |