FCDO Services

Job Description

Role Title	Governance and Assurance Manager		
Business Group	Business Services		
Job Family	Security		
Job Purpose	Lead and act as primary point of contact for governance and assurance (second line of defence) in respect of information and cyber security; assist in providing assurance and compliance of FCDO Services' systems with legal, national and local internal audit requirements		
Organisation Chart	See end of document		
Date Updated	29/05/2024	**Grade**	**C5**

KEY ACCOUNTABILITIES

- Collate assurance from system owners, operational cyber team and other stakeholders across the organisation to produce assurance reports primarily related to cyber security as part of the Senior Information Risk Owner (SIRO) reporting;
- Accountable for and monitoring of compliance to relevant policies, aligned to National Cyber Security Centre (NCSC) guidance, legislative and government standards and policies, and FCDO Services information security and cyber policies and strategies;
- Ownership and maintenance of required certifications and accreditations, including GovAssure, ISO27001 (owner of Statement of Applicability and ISMS Plan, facilitation of audit visits including setting up audit sessions, liaison with organisational stakeholders, including internal coordinator) and relevant sections of government inspections and audits;
- Act as Chief Information Security Officer (CISO) lead on the second line of defence in the internal information risk assurance framework, the Cyber Assurance Framework and provide active support on Secure by Design;
- Assist the governance and assurance group in general operation, monitoring and ensuring required reviews and caveats are completed as required;
- Support Lead Managers and Departmental Risk / Service Improvement Managers in identification and management of information security and cyber risks;

- Lead on governance, assurance and cyber security awareness across the organisation (not technical cyber specialisms) through regular communications, guest speakers, online training and training sessions;
- Co-ordination and provision of advice relating to Security Operating Procedures (SOPs) – ownership of standard wording of all SOPs; reviewer of all SOPs to ensure they align to policies within the remit of the Office of the Senior Information Risk Owner;
- Provide initial response and assist the CISO Team in respect of information security related incidents, coordinating responses and working with technical teams as required;
- Provide advice on IT security matters and information security requirements on new and existing ICT systems in line with organisational policy, risk appetite and latest legislation, regulatory and mandatory requirements;
- Work with internal stakeholders to develop relationships to help promote and improve information security and provide security advice on procurements, projects and new initiatives;
- To support the Team and wider Group Business Continuity requirements;
- Work with other security teams on training and updating staff on annual information security mandatory and ongoing training.

QUALIFICATIONS, KNOWLEDGE & EXPERIENCE

Essential:

- Good understanding of IT systems and associated risk management processes. Must be familiar with cloud and mobile technologies;
- Understanding of information security principles, relevant legislation, HMG IA Standards and ISO/IEC 27001;
- Appropriate professional qualification in relevant discipline e.g. CISM, CISMP, practitioner level certificate in 27001 or information risk management, or equivalent, etc.

Desirable:

- Track record of driving cyber security, information security and information assurance in public sector;
- Experience of working with assurance frameworks in relation to cyber and information security activities;
- Track record of influencing cyber and information security policy at national and organisational level.

CIVIL SERVICE BEHAVIOURS

Top three for job:

- Seeing the Big Picture.
- Communicating and Influencing.
- Developing Self and Others.

SUCCESS INDICATORS
Success measured and evidenced by: • Successful integration of role across all SIRO teams and wider security stakeholders across the organisation. • Production of reports of quality and value to the organisation. • Ascertainment of relevant certifications and accreditations in a timely manner. • Seen as authority in relevant lead areas.

Budget and Authority	N/A
Reports to: (Role Title and Grade)	Deputy Chief Information Security Officer
Direct Reports: (Number and grades of staff)	N/A

FCDO Services