Head of Information and Data Security

Department:	Cabinet Office
Section:	Modernisation and Digital
Reports to:	Strategic Director – Modernisation and Digital
JE Ref:	CB1011
Grade:	CS15 **JE Date**: 17/03/2023

Job purpose

The Head of Information & Data Security leads the framework that secures the Government of Jersey's information assets and IT infrastructure and ensures that information is managed in a way that meets regulatory and ethical requirements and security best practice, is protected from internal and external threats and malicious actors and supports GoJ's goals and objectives. The role provides leadership across the whole of GoJ in the areas of data subject rights, data privacy and information security and is accountable for the development of effective operational risk management.

Job specific outcomes

- Provide strategic oversight and wider professional leadership for all elements of the information management framework including information security, records management and data privacy/protection and builds capability and compliance across GoJ
- Provide leadership to the information governance, information security and technology operational risk teams, ensuring staff are developed to their full potential in their roles and performance management is embedded
- Own and manage the relationship and contract with the Data Protection Officer service provider ensuring maximum value to GoJ from the contract
- Develop, manage, maintain and evolve a delivery approach for information management, compliance and governance
- Prepare and provide strategic insight for the Chief Minister on information management and information security
- Develop, manage, maintain and evolve the technology operational risk framework and chair the M&D Risk Committee
- Provide advice, guidance and work collaboratively with transformational change programmes and initiatives to ensure they meet information governance requirements and meet GoJ digital ambition
- Act as the subject matter expert on information security across GoJ
- Lead the continuous monitoring and response to GoJ's information security maturity and the development of information security plans that improve the security posture, respond to changing cyber security threats and reduce the risk of impact from a cyber security incident

- Review, track and report on the financial and delivery performance of the information governance, information security and technology operational risk teams
- Be accountable for the design and delivery of a clear engagement and communications plan that raises awareness and promotes good information management and security practices
- Strategic ownership of cross departmental information governance and information security policies and procedures

Statutory responsibilities

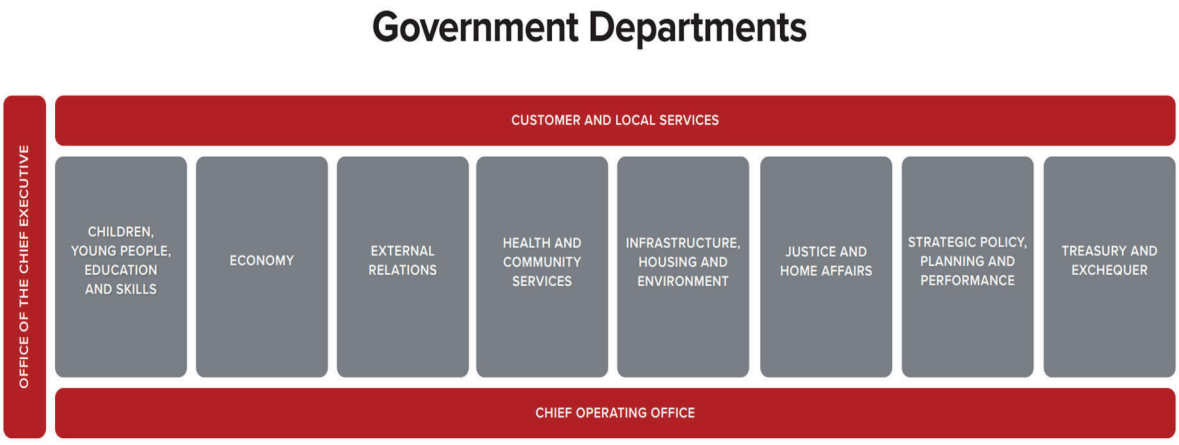
Active engagement, participation and compliance with any other statutory responsibilities applicable to the role, as amended from time to time.

This role is politically restricted. The jobholder is not permitted to undertake political activity involving standing for election to the States or as a Parish Constable, or publicly supporting someone who is standing for election or playing a public part in any political manner.

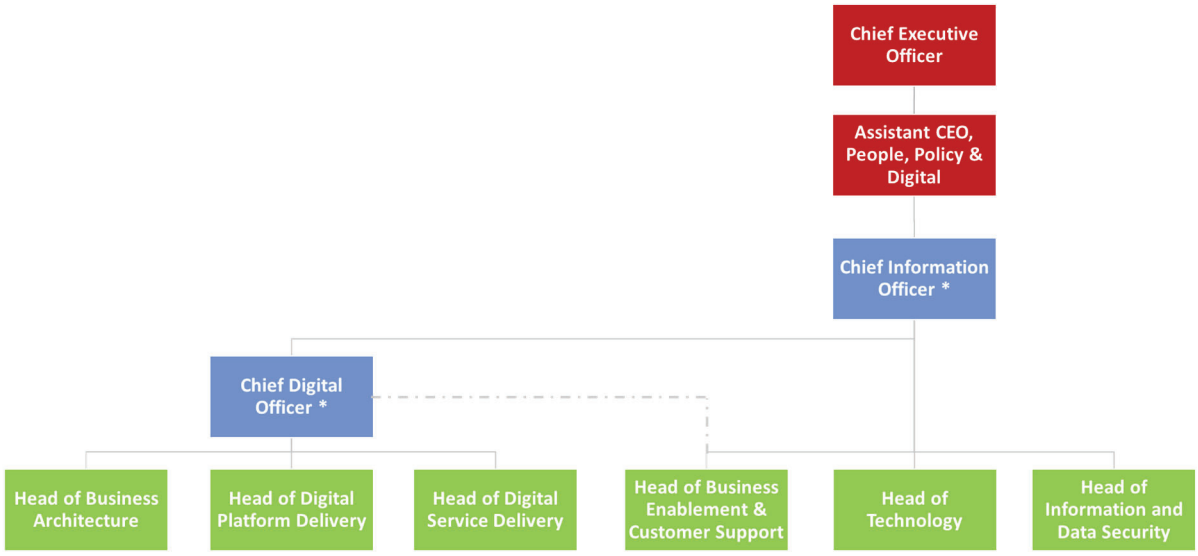
Services (TIER 1,2 and 3 jobs only-DELETE if not applicable)

- Privacy Management
- Technology Operational Risk Management
- Information Security

Organisational structure



Organisation chart



Person Specification

Specific to the role

Describe the knowledge, skills, experience, and qualifications required to perform the job to a satisfactory standard.

It is important to convey what the job requires, rather than what an individual might have, as these may be different. For example, you may have a postgraduate level qualification, however, an A' Level standard qualification is the requirement for the job.

ATTRIBUTES	ESSENTIAL	DESIRABLE
Qualifications *Please state the level of education and professional qualifications and / or specific occupational training required.*	Degree level qualification in an IT or business-related discipline or the ability to demonstrate the equivalent level of knowledge through experience. Extensive IT governance, risk, compliance, and / or related audit experience CISA, CRISC, CGEIT Certified or equivalent	PC.dp and/or PC.rm certification or equivalent
Knowledge *This relates to the level and breadth of practical knowledge **required** to do the job (e.g. the understanding of a defined system, practice, method or procedure).*	Demonstrated knowledge of: Industry wide information security frameworks including ISO 27001/2, NIST	Exceptional business acumen with a successful track record in aligning to business drivers Data Protection (Jersey) law 2018, Public Records (Jersey) Law 2002,
Technical / Work-based Skills *This relates to the skills specific to the job, e.g. language fluency, vehicle license etc.*	Demonstrable experience in: • Defining, establishing and delivering multiple aspects of a Governance, Risk and / or Compliance framework. • Contract negotiations including contract breach negotiations • Drawing strategic reports and recommendations from having the holistic view across a Department and Government. Drive decisions made from data, utilising an analytical skillset to leverage insights and analytics	
General Skills/Attributes	Strong verbal & written communication skills to	

This relates to more general characteristics required to do the job effectively, e.g. effective written communication skills, ability to delegate, motivation or commitment etc.	influence a wide range of stakeholders Must be a strong crossfunctional team player with ability to manage and coach others. Outstanding stakeholder management skills to establish and maintain strong working relationships. Leadership skills to enable multidiscipline teams to integrate with programme and project management disciplines and operational delivery teams. Broad technology knowledge with a proven understanding of legacy, current and emerging technologies and market trends.	
Experience *This is the proven record of experience and achievement in a field, profession or specialism.* *This could include a minimum period of experience in a defined area of work if required by an external body (for example a period of post-qualification experience).*	Extensive Demonstrable experience across: IT governance, risk, compliance, and / or audit experience Information Security Compliance and Assurance, Data and Records Management, Contract Management, Information Audit, Business Continuity, Staff Recruitment. Experience of establishing and improving sustainable programmes to meet regulatory or contractual requirements Extensive experience of Governance, Risk and Compliance Solutions	Previous experience in defining, establishing and delivering multiple aspects of a Governance, Risk and / or Compliance framework

Personal Attributes

Delete as appropriate:

Appointees to this role will be required to adhere to and perform their duties in line with the standards identified in the States of Jersey tier 1 to 3 core accountabilities, attributes and behaviour indicators.