IT, Data & InfoSec Lead - Financial Intelligence Unit (FIU) Jersey

Department: Economy

Division: FIU Jersey

Reports to: Chief of Staff & Capabilities FIU (Director's Office)

JE Reference: ECON1024

Grade: CS 9

JE Date: 21.03.2024

Job purpose

The post holder will take the lead on all FIU Technology, Data, Information Security and Business Continuity matters, including the operational use, delivery and suitability of core IT frameworks as well as the use and management of specialist databases, technology tools and enhancements. The core enabler for the FIU is technology and data. This role has responsibility for the data, IT infrastructure resilience and security management of all aspects. As such, this role is the critical enabler for all FIU operations and encompasses all aspects of information technology, information security and data management alongside source input and how to manage the systems and technology effectively. The primary role is to ensure useable data and IT infrastructure is always available to support the operational teams to deliver intelligence insight in a consistent, co-ordinated and systematic manner.

Job specific outcomes

Policy and Strategy

- Implement, own and deliver a technology and digital strategy for the FIU that is makes best use of data and technology solutions and is underpinned by information security and business continuity requirements to ensure the FIU is secure and can continue operations in case of incidents.

Technology

- Be the FIU lead on Information Technology, Systems and Sources and Information Security.
- Lead on the transformation of technology programme, working in collaboration with project managers and other FIU staff to demise existing systems and implement new ones, with relevant data migration and necessary operational protocols to enable better data access and manipulation for intelligence insight.
- Build a network of relevant experts to ensure that core systems (such as MS365), Egmont secure web, case management system, network analysis tools (such as i2), data manipulation tools and open-source aggregators are licensed and used efficiently across the FIU.
- Working with Director FIU and Head Business, Risk & Capabilties, implement risk management, security audit, information security and records management, ensuring visible, robust oversight and compliance with all governance requirements, thereby mitigating the risk of security incidents and/or legal action.

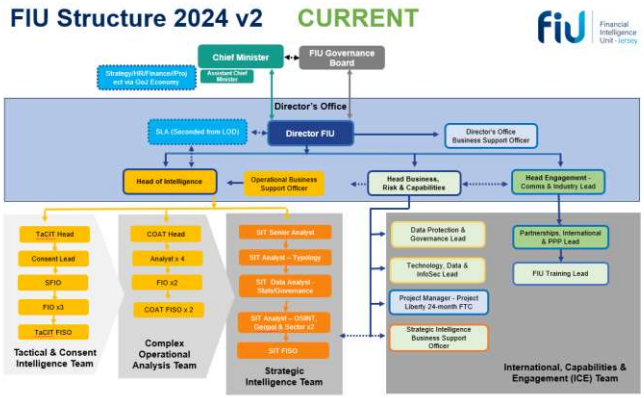
Information Security and Business Continuity

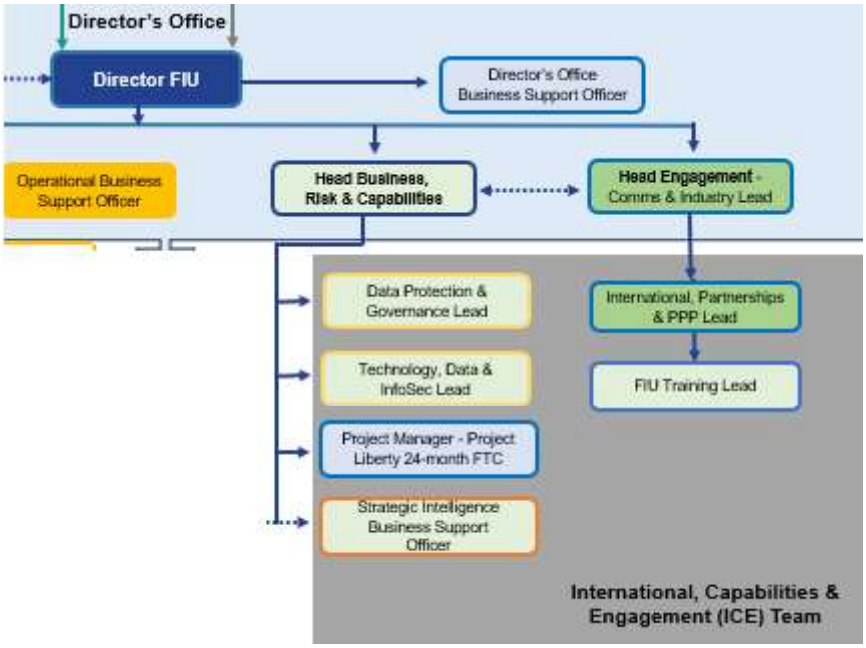
- The role requires close co-ordination with all teams and capabilities within the FIU to ensure policies and procedures are in place, adhered to and checked to identify, measure, monitor and mitigate information and cyber security risks in line with the FIUs internal risk management controls and those of its associated partners required to maintain accreditation to access and engage with law enforcement and UK agencies.
- Draft and deliver a full business continuity and disaster recovery governance programme, co-ordinated with other members of the Capabilities sub-team and relevant to an effective intelligence programme.
- Implement, manage and monitor all aspects of Information security, including but not limited to user access and data management and access, virus and malware defence and controls across all FIU platforms and IT.
- In association with partners, deliver clear guidance and management plans for the travel, storage and safety of all FIU IT and data.
- Develop and maintain an IT security risk register and ensure it is available for the Director's Office and any critical issues, breaches, risks or similar are raised at the earliest opportunities.
- Partner with a range of stakeholders across relevant partners within GoJ and other agencies to best manage the IT risk.

Statutory responsibilities

- Active engagement, participation, and compliance with any other statutory responsibilities applicable to the role, as amended from time to time.
- To work in accordance with the Data Protection (Jersey) Law

Organisation chart





Person Specification

Specific to the role

Personal Attributes - Appointees to this role will be required to adhere to and perform their duties in line with the standards identified in the Government of Jersey tier 4 core accountabilities attributes and behaviour indicators.

ATTRIBUTES	ESSENTIAL	DESIRABLE
Qualifications *Please state the level of education and professional qualifications and / or specific occupational training required.*	Degree/Level 6 or equivalent experience in any one of Information security, risk management, business continuity, data, finance, economics, business continuity, business fields or associated subjects. 5-7 years of general professional experience, including a minimum of 3 years in IT/Data/Business/financial crime/compliance/intelligence in either public or private sector. A portfolio of lower qualifications (Level 5 Diploma) on relevant subjects	Certified Information Systems Security Professional (CISSP) IT Security Officer course Business Continuity/Operational resilience qualifications
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).*	• Experience as a technology, InfoSec and/or Business continuity lead. • Experience manipulating structured and unstructured data sets to compile analysis and deliver data visualisation solutions. • Proven ability to utilise advanced knowledge, experience and judgement to analyse and interpret highly complex	Understanding of government information security processes. Knowledge of all aspects of corporate governance, including risk management, business continuity, information security.

	and multifaceted problems and to generate practical solutions. • Familiarity with case management tools, intelligence databases and/or network analytic tools (such as i2).	Familiarity with Artificial Intelligence and machine learning protocols, especially in the compliance arena. An understanding of the needs and challenges of working with intelligence data.
Technical / Work-based Skills	• Understanding of the internal structuring of data within different operating systems. • Offering first line, user advice on a range of platforms. • Understanding technical requirements for a range of technology solutions to be integrated across a wider network. • Organised; able to deal with multiple competing priorities and a high workload.	Understanding of risk assessments and action planning. Ability to challenge and negotiate with stakeholders to implement and adhere to legal and policy requirements and to improve performance; willing to lead challenging conversations where necessary. Developed business and reasoning skills, with evidence of working at pace in a complex multi-stakeholder environment to design and implement governance, operational and improvement programmes.
General Skills/Attributes	• Resilient, maintaining effectiveness under pressure. • Ability to work independently and autonomously.	Capable presentation and communication skills to transmit complex, sensitive or detailed information
Experience	• Experience of devising and implementing robust corporate governance systems that relate to IT. • InfoSec/IT/Data/Business Continuity manager. • Experience of representing the views of senior managers to ensure that organisational policy, political, and communications priorities are fully understood by internal stakeholders.	Understanding of intelligence and financial crime challenges. Experience of successfully leading the development of delivery plans to meet strategic priorities
	The post holder is required to undergo SoJP Jersey vetting and UK National Security Vetting to a minimum of Security Clearance level.	