|  |  |
| --- | --- |
| **Position title** | UK Business Information Security Officer |
| **Date** | 28th May 2025 |
| **Line Manager title** | UK Director of Technology Operations |
| **Grade** | 6 |

| Purpose |
| --- |
|  |
| SUEZ UK is looking for a Business Information Security Officer (BISO) to lead a small UK team and take responsibility for the level of Cyber Security and Defence in the UK working with the UK Director of Technology Operations, the Group Chief Information Security Officer and the Group Cyber Security Department utilising group policies, standards and services as appropriate to meet UK legislation and cyber security best practice.This role represents the CISO on all security matters in the UK and will be accountable to both the UK Director of Technology Operations and Group CISO for deploying the group Cyber Risk Policy including integrating security across the whole of the UK Technology services (IT and OT) and attaining / maintaining UK Cyber Essentials Plus accreditation.The France BISO is taking on cross European activities and therefore is looking for this role to Expand in time to a Deputy European BISO. |

| Key Responsibilities |
| --- |
|  |
| Main Responsibilities and Duties of the UK R&R BISO will include:* Organise the implementation of cyber policies by prioritising the most critical assets for the business, in both IT and OT industrial perimeters:
	+ Identification and mapping of technology assets,
	+ Analysis of security gaps and asset risks,
	+ Monitoring the implementation of associated remediation plans.
* Activate & integrate cybersecurity “by design” in all technology projects, in particular:
	+ Risk analysis and definition of associated mitigation measures,
	+ Ensuring that these mitigation measures are properly implemented, and validating them for any project involving critical assets,
* Monitor the performance of cybersecurity suppliers and services, ensure Cyber Security Insurance is appropriate to meet UK requirements
* Act as an interface and facilitator between the UK Business and Technology Units and other teams in the group cyber department
* Complete the annual Cyber maturity self-assessment, define the associated action plans, monitor and deliver their implementation
* Monitor Cyber indicators and track their implementation,
* Participate in the management of major Cyber incidents and crisis concerning technology assets, monitor and implement associated action plans,
* Raise awareness of Cyber risks, particularly among Division/UK top management and Technology contacts (development security, application security, etc.)
* Help improve the OT / industrial cyber security in the UK, share lessons learned across Europe
* Deploy a Cyber Essentials Plus program to address all in scope services across the UK, Participate in the European NIS2 program as appropriate.
* Act as the UK Business Unit’s Cybersecurity contact, within the framework of integrated Cyber governance including Data Privacy, Ethics & Compliance, Environmental & industrial risks and Safety,
* Take part as needed in regular meetings to review risks and associated action plans with the R&R Division's COMEX sponsors,
 |

| Skills |
| --- |
|  |
| * Extensive experience in leading IT Security activities in complex, multi-site environments that have operational technology elements
* Able to reinvent process where this is falling short, and to influence adoption of such processes across the organisation and at all levels.
* A collaborative team player with a positive attitude to meeting and exceeding business demands
* A broad and in-depth technical knowledge across the cyber aspects of networking, hosting (on premise and cloud), telephony, access & identity.
* An excellent people leader able to develop and manage resources working across several technical disciplines and with competing demands effectively, including those working remotely
* An effective communicator who readily reports progress on work to business and Technology leadership as required
* Excellent vendor management, driving value through contracts and ensuring tender activity and other procurement processes, are completed in good time, and in line with policy.
* Can utilise project management resource effectively to deliver complex change programmes in the security space
* Creates training material and other resources to influence user behaviour for adoption of security policy and process
* Ability to lead major security major incidents and play a part in resilience activities and the creation of business continuity artefacts
 |

| Behaviours |
| --- |
|  |
| Actively embraces the global SUEZ Leadership Behaviours and Group Values by demonstrating:* **Shape the Future:** Put our clients at the centre of our actions, design an actionable vision, make sustainability a key differentiator, Dare to innovate and drive continuous improvement.
* **Make it Happen:** Dare to drive change, be exemplary to aim for success.
* **Collaborate to Elevate:** Always lead in the Groups best interests, Foster Transparency & Networks
* **Unleash the talent of your People;** Trust & delegate, allow each person to grow, Care for yourself & others.
* **Team Spirit**: Together, we work, we collaborate, we problem solve, we support, we encourage, and we celebrate.
* **Respect:** We care, we can be our authentic selves, we’re compassionate, we’re ethical and we’re honest. We act to keep everyone safe and well.
* **Commitment to the Environment:** We preserve, restore and protect our planet. We act to reduce, reuse, recycle and recover resources.
* **Customer Focus:** We’re dedicated, focused and creative. We innovate, we advocate, and we collaborate with our customers for the environment.
* **Continuous Improvement:** **Demonstrate a proactive and collaborative approach to identify and implement opportunities which continually improve business processes, quality and overall performance.**
 |

| Knowledge |
| --- |
|  |
| * The candidate must have a minimum of 5 years' professional experience in IT, cyber or industrial risk management.
* The BISO must have a sound knowledge of risk management, compliance frameworks, integrating security into projects, developing and monitoring indicators and executing action plans.
* Ability to summarise and communicate, interpersonal skills and a sense of mentoring are assets for this position, which involves interaction with both IT and operational business teams.
* Knowledge of Cyber Essentials, Cyber Essentials Plus and / or the NIS2 Directive and the successful implementation of these in an industrial or service setting
* A practical understanding of ISO27001, NIST-800, Waterfall and Agile project and change management principles and methodologies such as PRINCE2, Six Sigma. Agile, Scrum etc
* Excellent budget and cost management skills across both OPEX and CAPEX
* A good level of French would be beneficial but not essential
 |

| Specific candidate requirements |
| --- |
|  |
| * Significant experience with business management and a working knowledge of information security risk management and cybersecurity technologies and strategy
* Strong understanding of Windows, Linux, virtualisation, and networking concepts
* Familiarity with industry security standards including NIST, ISO, SANS, COBIT, CERT
* Familiarity with current data privacy regulations, including GDPR and regional standards.
* Strong understanding and experience with Secure SDLC and DevSecOps or security automation
* Capable of understanding and communicating the business and profit impact that infosec operations have on the organisation
 |

| Qualifications |
| --- |
|  |
| * A Computer Science Degree (or other relevant subject) or equivalent professional experience
* CISSP (Certified Information Systems Security Professional)
* Microsoft certifications and/or network qualifications
* ITIL Foundation
 |