babcock™

Factsheet

Information & Cyber Security

The Information and Cyber Security function within Babcock provides governance, direction, policy and assurance on all information and cyber security matters. This is achieved through the delivery of security operations, information assurance, audit and compliance activities as well as guidance and support across Babcock.

The Information and Cyber security team provide protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Cyber Resilience

Cyber resilience is key to Babcock in protecting the information systems, networks, and data that we own and maintain. The team has responsibility for detecting and responding to cyber-attacks alongside carrying out detailed **monitoring, alerting and analysis**.

A proactive approach is taken to identify **vulnerabilities** and support early remediation as well as carrying out **threat intelligence** reporting in conjunction with external agencies and other industry partners.

Incident response is a key aspect; CSIRT (Cyber security incident response team) plans are **tested regularly**, with lessons learned recorded and actioned. **Incident investigation, malware** and **forensic analysis capability** exists to ensure that any potential issues are fully documented and handled without affecting evidence. **Penetration testing** is a further capability, and this is complemented with external 'Check' services to meet stakeholder requirements. Third party security support is offered for access to Babcock resources.

Information Assurance

Information assurance is provided through protecting the confidentiality, integrity and availability of information. This is achieved through **policy and procedures** formulation, maintenance and publication.

Key highlights

- Certifications
  - ISO27001 – Information Security
  - ISO 22301 – Business Continuity
  - UK Cyber Essentials Plus
- Approvals to hold and process government information in relevant countries in which we operate
- Full SOC Protection, Detection, Monitoring and Response Capability
- Skilled teams with security certifications including CISSP, CISM, CISMP, CCRMP, ISO Audit, BTL1, GCTI, CompTIA Security +, CompTIA Pentest +, CREST Trainee Penetration Tester
- Cryptographic controls capability
- Data protection and privacy expertise
- Audit and Compliance capability
- Leadership and governance through CISO, CIO and Executive structure
- Cyber and Information Security policy and procedures
- Through-life Risk Management for all systems, networks and information assets
- Support to contracts and supply chain through policy and ongoing assessment

Contact us:
Email: sustainability@babcockinternational.com
www.babcockinternational.com/sustainability

Published 10.11.2023

Risk management processes include assessment / reporting to ensure Babcock risk appetite is maintained. A register of information assets and the associated risk assessments is maintained and reviewed on a quarterly basis with Senior Information Risk Owners (SIROs)

Supply chain security is key in protecting information and communications, flowing down certification / controls requirements, and working closely with Procurement and Supply Chain teams.

Incident management is a key process and includes a formal approach to response, reporting and follow up of incidents raised. The process comprises the requirement to report to external stakeholders in a timely manner e.g., ICO and other stakeholders.

The function also reviews and advises on technical controls, vulnerabilities and provides **change approvals** as part of project and programme activities including those necessary for IT systems implementation and upgrades. Support is provided to projects and contracts to meet security requirements related to handling of personal and sensitive information including the completion and review of business and data protection impact assessments.

Certification in Information Security (ISO27001) for the IT function is held and maintained, enabling continual improvement, metrics measurement, review and overall leadership from the Babcock Executive.

Cryptographic controls are necessary to protect sensitive information and procedures including regular audit are in place to maintain and protect cryptographic materials.

A policy and robust processes are in place for approval of **international travel** to protect export of controlled or sensitive government information. The function maintains a register and provides approvals.

Certification is held for **Business Continuity** of the IT function (ISO22301). This includes regular tests and table top exercises.

Specific assurance is necessary for handling of **government information** across multiple countries and support is provided in meeting standards set by governments globally. Threat / risk assessment, controls and mitigations are established and maintained through-life to achieve and maintain accreditations for networks, systems and information used in delivery or government contracts. Data Centres have been externally assessed and assured to handle classified information. Staff are vetted and cleared to handle government sensitive information including national caveats.

A **data retention** policy is held to meet the needs of the multiple regulatory and contractual requirements. The function also ensures sanitisation of used devices for re-use where appropriate. The **privacy policy** also protects personally identifiable information (PII) and subject access requests are reviewed and a register maintained.

The function carries out **education and awareness** across Babcock through mandatory and additional training of all our IT enabled workforce on cyber security awareness, data protection, trade controls and anti-bribery and corruption. Staff have access to a Security Knowledge Zone which provides regularly updated advice and guidance. Further details on mandatory training can be found in the Governance section of the Annual Report.

A full **audit and compliance capability** is delivered. The audit strategy and plan ensures delivery of ISO27001 / ISO22301 certification, compliance with policy, technical vulnerability checks and management of external audits including financial, SWIFT etc.

Leadership and governance of the function is provided by the Chief Information Security Officer (CISO) who reports to the Chief Information Officer (CIO), a member of the Babcock Executive. A quarterly Information Security Committee with Executive representation is held to provide governance, direction and assurance that the Babcock security posture is appropriate and that Babcock's reputation and employees, customers and other stakeholders are protected.

Contact us:
Email: sustainability@babcockinternational.com
www.babcockinternational.com/sustainability

Published 10.11.2023