Curriculum Vitae - Leigh

Professional, Driven, Positive

e3e5ada@datadefence.pro +44 (0)7492 061234 https://datadefence.pro/

Information Security Manager

Profile

Passionate about information security and a trusted Information Security Manager. Successful in creating, leading and maintaining Information and cyber policies, risk management strategies and training materials – including delivery. Adept at closing critical loopholes maximising security options and staying ahead of current threats. Exceptional program manager, and aligned with the challenges faced by senior management. Managing risk, ISO27001 certifications, Cyber Essentials and PCI-DSS to ensure the entire spectrum of governance, risk and compliance is in place and effective. Presented as a guest speaker at an ISACA seminar, and gained seven separate ISO27001:2013 certifications for Information Security Management Systems I had created.

Professional Experience

Company 2

Active in creation of new policies and processes recommending amendments. Initiated a company-wide cyber awareness campaign, delivering with passion and encouraging others to the extent that they willingly volunteered as cyber awareness champions for their teams.
Creation and development of cyber awareness materials consistent with NCSC, developing processes for simulated phishing tests.
Strongly developed cyber response capability – including Business Continuity Planning.
Developed an information security team consisting of three other people to improve the security posture of the organisation.
Introduced NIST cyber security, NIST 800-53 controls and risk management frameworks to the organisation, and set them to work for security risk management.
Introduced and deployed third-party risk questionnaire and evidence system, including work on supplier management policies and processes.
Wrote and deployed a vulnerability management process that included scanning, treatment and senior management review and action plan for discovered vulnerabilities.

Company 1

Active in evaluation and approval of testing and implementation of technical changes and upgrades to key business systems; introducing a new change management risk assessment.
Planned, scheduled, communicated and executed a full risk-based audit program that incorporates both ISO27001and company internal controls.
Accustomed to working with all areas of the business at all levels on the Information Security Management System (ISMS), and trained top management and business managers in the processes involved in establishing, implementing, operating, monitoring, reviewing and improving their ISMS.
Developed awareness materials and presentations to present to the non-technical side of the business, explaining complex technical concepts in straightforward terms.

Work Experience

Dates	Organisation	Role
September 2023 - Current	None	Short employment break
July 2022 – September 2023	Company 2	Information Security Manager
May 2022 – July 2022	None	Short employment break
December 2010 – February 2022	Company 1 (Acquired co 0)	Information Security Manager
April 2008 – December 2010	Company 0	Systems Support/Systems Analyst

Key Qualifications

- Certified Information Security Manager (ISACA Gold membership)
- ISO27001:2013 Lead Auditor
- ITIL v3 Practitioner
- BSc (Hons) Network Computing
- Higher National Diploma (HND) Computing Support
- Working towards:
- ISACA CRISC (Certified in Risk and Information Systems Control) – currently studying
- Lead Auditor ISO/IEC27001:2022, ISO/IEC27002:2022
- NIST Lead Implementer Certification

Leads, produces and delivers innovative solutions including (but not restricted to) the following:

- **Information Security Governance**
  - Created / maintained information security policies and processes as agreed by management, as well as cyber security incident and communications response plans and reporting templates to NIST, CIS and other industry standards.
  - Maintenance and continual improvement of Managed Systems with focus on NIST and ISO27001:2022 ISMS (Information Security Management System); resulting in consistently high audit results throughout my information security career.
  - Successfully maintaining certification of IT services, including ISO27001, Cyber Essentials Plus.

- **Information Risk Management**
  - Creating and maintaining the regional information security risk management structure and processes to ISO27005, NIST, company and industry standards
  - Training IT and business stake holders on risk management strategies and procedures, and reinforcing the importance of asset management and valuation.
  - Hosting internal Security Working Group meetings, contributing effectively to external meetings where required. With a focus on privacy and protection of our colleague and customer data, strengthening defences and strategies for compliance with GDPR and UK data protection law.
  - Led and realised risk management in IT projects involving third-parties, introducing strict supplier qualification strategies and materials where there were none. This has lowered the risk profile and attack surface of strategic projects significantly.

- **Information Security Programme Development and Management**
  - Leading information security programmes, such as six successful ISO27001:2013 certification projects simultaneously resulting in a ‘first-time’ certification for each. This included training and awarding local certificates for ISMS Managers whom I had trained using my own material.
  - Using threat intelligence / modelling, risk and incident analysis to write, produce and deliver information security awareness and training packages, for individual job roles and changing with the announcement of new threats. Setting up a network of ‘security champions’ to spread awareness.
  - Undertaking a programme of compliance and improvement of the PCI-DSS compliance framework within our PCI estate, and that of our subsidiary companies.

- **Information Security Incident Management**
  - Devises innovative incident management strategies that included Business Continuity.
  - Recommends, prepares, implements detection and analysis, containment, eradication, recovery and post-incident activity strategies for response to information security incidents.
  - Respond to serious information security incidents invoking new strategies
  - Liaise with all affected parties to their satisfaction.
  - Created corrective actions for the departments concerned as part of the post-incident activity strategy – continuing follow up their progress for each incident.
  - Working with industry managed service providers to control SOC and SIEM activity, using Splunk and Microsoft Defender 365.