NCSC Certified Training - Cyber Security for Data Asset Owners

Maritemex
Holistic Cyber Security Resilience

1. COURSE

Ce séminaire est consacré à :

- Knowledge and understanding of why Cyber Security is critical to business
- The importance of the role of the Data Asset Owner (DAO)
- Increase in awareness of Government and Industry best practice and standards
- Awareness of the multiple threats and consequences (both external and internal) including evolving trends
- An overview of current and forthcoming laws, legal rights and responsibilities that are expected and required of DAOs
- Government and Industry best practice on: Strategy and Governance, Information
- Assurance
- Information Risk Management including Risk Appetite and how to create and manage Risk
- Balance Cases (RBCs)
- Understanding and advice regarding best practices in relation to metrics and reporting
- Incident Management and Business Continuity
- The confidence to deal with issues through application of real-world case studies and Scenarios

2. COURSE CONTENT

The position of Data Asset Owners (DAOs) is key in an organisation's quest to manage Information Risk. Cyber Security and Information Assurance is not just an issue for the IT Department; leadership by DAOs is critical to promoting the right culture within an organisation to exploit, manage and protect information effectively.
This comprehensive one-day course is aimed at DAOs and for senior managers with responsibility for protecting and exploiting critical business information. Training delegates will be provided with a safe and stimulating forum to discuss key issues and challenges, along with examples of best practice in Cyber Security and Information Assurance. The course will equip DAOs with in-depth knowledge and opportunities to apply their learning through real-world case studies and to effect change in their role immediately and uniquely in relation to their organisation.

3. COURSE FORMAT

Learners will engage in an interactive workshop which will allow them to develop theoretical knowledge and apply it to their own situations. Delivery will be through a blended approach that will allow learners to fully engage in the session and gain practical examples of how to turn theory into practice.

4. DETAILED COURSE PROGRAM (unrolled training sequences)

Session	Delivery
1	***Inrodaction***
2	***Threats and Vulnerabilities*** The increasing and evolving threat landscape along with the current context
3	***Understanding and Impact on Business*** Developing a clear understanding of why holistic Cyber Security is important and understanding the roles and responsibilities across an organisation and external stakeholders
4	***The Law and Standards*** Looking at the law and international legislation, regulation and standards with a clear link to individual responsibilities; and understanding consequences of breaches and non-compliance
5	***Organisational Leadership and Governance*** Reviewing the best practice examples of the use of Data Asset Owners, management of information assets, Cyber risk and Information Assurance
6	***Building Cyber Resilience and Incident Management*** A practical review of how you transfer theory into practice within an organisation
7	***Course Summary and Evaluation***

5. COURSE PREPARATION

Learners should be familiar with their organisation's Policies and Procedures and demonstrate a commitment to developing their understanding of owning and protecting valuable information assets.

6. EVALUATION DU COURS

Participant engagement and contribution is essential in this course. It is expected that all learners fully interact with the learning and the group activities.

7. BIOGRAPHY

All course tutors will have the following professional credentials.

- UK National Cyber Security Centre Certified Trainers
- Higher level professional and teaching qualifications, gained over a career in Cyber Security practice.
- Contribution to the profession, giving back to the community at large, through voluntary engagement and seats on esteemed industry panels, working groups and special interest groups.
- Wide experience of professional roles in Cyber Security, leading to national and in many cases
- international reputations in domain.
- A complete and extended understanding of Cyber Security, Information Governance across a number of sectors
- A wide-ranging understanding of Cyber Security laws the related legislation surrounding
- international expectations

Our experienced, expert and engaging NCSC and Executive Trainer pool includes the following profiles:

- **NCSC Certified and Executive Trainer:** Experienced strategy adviser and solution implementer, with international leadership experience in both government and commercial organisations. Over 22 years' experience in the fields of Cyber Security, Information Assurance and Information and Communications Technology after a background in Computer Science and Computing Information Systems. A Visiting Teacher of Cyber Security at the Oxford Martin School of Oxford University. Leads on audits and compliance-related activities with a focus on Critical National

Infrastructure, including Central Government and Law Enforcement.

- **NCSC Certified Executive Trainer:** Extensive financial services sector, developing Cyber Security and Information Assurance strategies, delivering Board briefings, leading audits and training and mentoring Senior Executives. Clients include G7 banks, central banks, retail banks and private equity firms. A thought leader in the area of Cyber Security and Information Assurance, speaking at conferences with articles regularly published. A visiting Professor at Oxford University.

- **NCSC Certified and Executive Trainer:** Extensive experience includes mentoring Senior Executives in both the private and public sector. An established and highly effective leader with operational and commercial experience spanning private and defence sectors in the UK, Europe and the Middle East. Led Cyber Health Checks and Audits for multi-national clients, identifying key Cyber risks and threats and advising on improving Cyber resilience.

- **NCSC Certified and Executive Trainer:** Expertise and experience in delivering training and workshops to Board and senior audiences across government and the commercial sector. Background includes geopolitical risk and global threats, information risk and security, as well as risk mitigation, crisis management and prevention. Fostered networks for sharing best practice with Cyber Security organisations in the US, the EU and across the Commonwealth and was a member of the Cyber Assessment Advisory Panel at the UK National Cyber Security Centre (NCSC).

- **NCSC Certified and Executive Trainer: c**oaches and trains leadership on Cyber and Risk across sectors and in the Critical National Infrastructure. Brings significant operational and field experience to his practitioner and academic work and specialises in the human dimension of cyber security. Previously, he was Chief Executive of a UK national body and author of a number of Cyber Security books sold internationally.

- **NCSC Certified and Executive Trainer:** Experience of wide ranging oganisational support. Advises on information governance policy development and Cyber Security leadership and strategy. Background in education, academia and the not-for-profit sector has seen him advise government on national skills strategies and develop skills programmes in Cyber Security across the UK. Vice Chairman of the Information Assurance and Advisory Council. Working with national and regional bodies, and private sector parties, he focuses on developing regional cyber resilience strategy. Recipient of a National Cyber Security Award for his work with young people and cyber security.