Information Security for Executives

Understand your organisation's information security challenges and proactively align your response to balance value and risk

Information and information technology systems are critical to business success, and an effective approach to information security is key, however businesses globally face significant challenges implementing and maintaining the right approach to security, and we are seeing almost weekly news of the big businesses suffering security breaches.

Executives and Directors are becoming increasingly aware that they have a key role in ensuring an appropriate information security framework is in place. This helps ensure alignment with business goals and objectives, and is essential for prevention, detection and response to incidents.

This half-day workshop provides introductory and practical coverage of information security for business executives. Using relevant scenarios and case studies, this workshop will help Executives respond to the security challenges they face and understand their role in the information security framework.

Who Should Attend

- Business Executives
- Directors
- Senior Managers
- Risk Practitioners
- Chief Risk officers (CROs), CIOs, CISO
- Information Security Managers
- IT Audit and Assurance professionals
- other IT Risk Management professionals

Learning Outcomes

- Gain a understanding of information security for your business context
- Gain a high-level understanding of the various security risks and threats facing organisations today
- Understand the differences between, and accountabilities for, governance and management of information security
- Develop the knowledge and skills required to understand your role in your organisation's information security framework
- Understand the components of an effective information security program, and how to align them with your business needs
- Acquire the necessary insights to support an Information Security Management System
- Understand how to gain value from the various best practice guidance and standards that exist.

Course Contents

Session 1: Overview of Information Security

- Defining information security
- Identifying information security goals for your business
- Separating information security governance and management

Session 2: Todays Information Security Challenges

- Understanding the security implications of your business transformation agenda
- Understanding information security in the extended enterprise (i.e. business partners, service providers and vendors)
- Understanding emerging technologies and their impact on security
- Exploring the techniques used by hackers to breach IT systems

Session 3: Introduction to Risk Management

- Overview of risk frameworks and standards (COBIT 5 for Risk and ISO 31000:2009, Risk management – Principles and guidelines)
- Understanding the Risk Management lifecycle:
  - Risk Identification, Assessment and Evaluation
  - Risk Reporting
  - Risk Monitoring
- Understanding techniques for security controls' monitoring and maintenance

Session 3: Implementing an effective Information Security Framework

- Identifying the positive and negative security scenarios impacting your business
- Developing an effective security strategy:
  - Identifying the required security capabilities and resourcing options.
  - Identifying regulatory, compliance and third party security requirements.
- Implementing effective security governance
  - Implement risk and control reporting ("dashboards"), strategy review, security program governance practices.
- Implementing an Information Security Management System.
- Establishing a deliberate security culture
- Enhancing business resilience and response
- Establishing effective security monitoring
- Establishing assurance processes (control self-assessment, internal audit, testing cycles, external audit, certification)
- Understand how to gain value from the various best practice guidance and standards that exist.