AUSCERT
Australian Cyber Emergency Response Team

W auscert.org.au
E membership@auscert.org.au
P +61 7 3365 4417

AusCERT Cyber Security for Risk Practitioners Training – Overview

About this Course

Risk professionals have a thorough understanding of risk management processes but may not have a comprehensive awareness of cyber security issues. This course is designed to empower risk practitioners to effectively and confidently engage with cyber security professionals and to integrate cyber security risks into enterprise risk management processes.

Required Background Knowledge

- An understanding of risk management principles
- Practical experience performing risk management processes such as risk assessments

Learning Objectives

Upon completion of this training course, participants will:

- Have improved confidence to effectively liaise with IT and cyber security professionals
- Understand fundamental information security principles
- Have an appreciation of the current cyber threat landscape
- Understand how to identify cyber security risks to business objectives
- Increased awareness of where to find helpful information security resources
- Have improved confidence in discussing cyber risk with executives
- Increased ability to support the integration of cyber risks into the organisation's governance and management approaches
- Gain the Confidence to perform a risk assessment of cyber security risks

Approach

- Provide a broad perspective on the field of cyber security and the relation to risk management
- Facilitate opportunities for participants to share experiences and knowledge
- Provide relevant and pragmatic examples of cyber security risk management in practice
- Explicit focus on flexibility and time for participants to ask questions and apply knowledge with case study examples
- Practical application of new knowledge with a scenario-based risk workshop, identifying and analysing cyber risks

Curriculum Outline

- Fundamental cyber security terminology
- Introduction to the current cyber threat landscape
- Cyber security specifics in the identification and analysis phases of a risk assessment
- Risk assessments for different purposes – management reporting and security planning
- Differences between risk assessments, threat assessments and vulnerability assessments
- Capability maturity model for cyber security
- Standard risk assessment techniques and their application to the cyber risk context:
    - identification
    - analysis
    - evaluation
- Traps and pitfalls when applying risk management to cyber security risks
- Summarisation of detailed risks in a format and language suitable for executive audiences
- Case study workshop – focused on risk analysis in the cyber security context
- Open discussion – Q&A