

Cyber Security Risk Management – Overview

About this Course

This course is designed to provide participants the confidence to perform a risk assessment of cyber security risks, the ability to rate, assess and report business risks rather than technical vulnerabilities. Calibrating cyber security as business risks rather than technical vulnerability severity readily facilitates business leader buy-in.

Required Background Knowledge

- There are no particular background knowledge requirements for this course.

Learning Objectives

- Enhance understanding of how to identify and assess cyber security risks to your organisation
- Management of cyber security risk using standards-based risk management processes
- Integration of cyber security risk management into organisational governance and management processes
- Increase confidence to perform a risk assessment of cyber security risks
- Enable IT and cyber security professionals to liaise with risk professionals to report up to boards and executives
- Use business risk to set priorities for your cyber security improvement program

Approach

- Provide a broad perspective on the field of information and cyber security and the relation to risk management
- Facilitate opportunities for participants to share experiences and knowledge
- A mix of theory and engaging learning experiences including quizzes, and group discussions
- Provide relevant and pragmatic examples of cyber security risk management in practice
- Embed learning through practical risk management workshop exercise

Curriculum Outline

- Fundamental risk management terminology and process (ISO 31000 and ISO 27005)
- Application of standard corporate risk management frameworks to cyber security risks
- Techniques for each phase of cyber security risk management:
 - identification
 - analysis
 - evaluation
 - reporting
- Risk management as a framework for sound decision support
- Traps and pitfalls when applying risk management to cyber security risks
- Workshop – put the theory into practice