

ISYS90018 E Risk Assessment

Credit Points:	12.50
Level:	9 (Graduate/Postgraduate)
Dates & Locations:	2010, Hawthorn This subject commences in the following study period/s: Semester 1, Hawthorn - Taught on campus. Semester 2, Hawthorn - Taught on campus. Please refer to MCCP website. www.mccp.unimelb.edu.au
Time Commitment:	Contact Hours: 24 hours of face-to-face contact over an eight-week semester plus at least eight hours of pre-seminar reading. Total Time Commitment: It is anticipated that students will need to allocate around 100 hours to undertake the assessable components of the subject.
Prerequisites:	nil
Corequisites:	nil
Recommended Background Knowledge:	nil
Non Allowed Subjects:	nil
Core Participation Requirements:	For the purposes of considering requests for Reasonable Adjustments under the Disability Standards for Education (Cwth 2005), and Students Experiencing Academic Disadvantage Policy, academic requirements for this subject are articulated in the Subject Description, Subject Objectives, Generic Skills and Assessment Requirements of this entry. The University is dedicated to provide support to those with special requirements. Further details on the disability support scheme can be found at the Disability Liaison Unit website: http://www.services.unimelb.edu.au/disability/
Contact:	Melbourne Consulting and Custom Programs Level 3, 442 Auburn Rd Hawthorn VIC 3122 Phone: 03 9810 3300 Email: mccp.enquiries@mccp.unimelb.edu.au
Subject Overview:	This subject examines the role of risk driven methodologies in modern information security environments. It covers the risk management lifecycle and develops an understanding of security risk management in an organisational context. It provides the fundamental principles of information security and how security processes are implemented in organisations. It includes the concept of risk management, how to conduct risk assessments and how they can be used to better create a secure organisational environment.
Objectives:	Students who successfully complete this subject will have demonstrated an understanding of: <ul style="list-style-type: none"> • The theoretical framework and methodologies applied in information security risk assessment particularly in the business environment; • Fraud and internet usage management as part of business practice; • Practical application of risk mitigation strategies in IT environments.
Assessment:	Up to two written assignments totalling 4000 words.
Prescribed Texts:	nil
Breadth Options:	This subject is not available as a breadth subject.
Fees Information:	Subject EFTSL, Level, Discipline & Census Date, http://enrolment.unimelb.edu.au/fees
Generic Skills:	The essential elements to be covered are:- <ul style="list-style-type: none"> # the meaning of 'information security' and how modern information security management is driven by a risk-based approach

	<ul style="list-style-type: none"># the need for information security in organisations including threat categories and attacks in information security# information security risk assessments,# the various stages of information security risk management including identification, analysis, evaluation and treatment# the role of risk standards, audits and assessments in information security management
Links to further information:	http://www.mccp.unimelb.edu.au/courses/award-courses/graduate-certificate/digital-forensics