ITEC854

Security Management

S2 Evening 2017

Dept of Computing

Contents

General Information

Unit convenor and teaching staff
Unit Convenor
Milton Baar
milton.baar@mq.edu.au
Contact via milton.baar@mq.edu.au

Credit points
4

Prerequisites
Admission to MInfoTech or MEng or MSc

Corequisites

Co-badged status

Unit description
The intent of this unit is to provide students with a working knowledge of commercial information security governance requirements, tools and techniques. The unit has a practical focus with tutorial and laboratory work that will include aspects of physical security and hacking, information security architectures and the creation of a dummy company on which the tools and techniques will be developed and tested. Topics include an introduction to information security, standard and governance, risk management concepts, security threats, controls, practical hacking, server hardening, evidence collection, business community planning and DRP, creating an enterprise information security framework, and EISF/ISMS certification.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

On successful completion of this unit, you will be able to:

Describe and explain the differences between security frameworks and standards

Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk

Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment

Identify and analyse basic configuration errors and basic exposures; assess hacking/ hardening techniques and their suitability as controls

Assessment Tasks

Name	Weighting	Hurdle	Due
Quiz 1	10%	No	22/8/2017
Lab work review	20%	No	3/10/2017
Quiz 2	10%	No	3/10/2017
Assignment	20%	No	7/11/2017
Quiz 3	10%	No	31/10/2017
Industry presentation	30%	No	7/11/2017

Quiz 1

Due: **22/8/2017**
Weighting: **10%**

The multiple choice quiz has a time limit of 30 minutes and is conducted online using iLearn. It will cover the material in lectures from weeks 1-4 inclusive.

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk

Lab work review

Due: **3/10/2017**
Weighting: **20%**

This is due to be handed in at the end of the last week of the mid-semester break. It is an assessment of your group work in the labs and every group member will receive an individual mark combined with a group mark.

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk

- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic configuration errors and basic exposures; assess hacking/ hardening techniques and their suitability as controls

Quiz 2

Due: **3/10/2017**
Weighting: **10%**

The short answer quiz has a time limit of 45 minutes and is conducted online using iLearn. It will cover the material in lectures from weeks 5-8 inclusive.

On successful completion you will be able to:

- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic configuration errors and basic exposures; assess hacking/ hardening techniques and their suitability as controls

Assignment

Due: **7/11/2017**
Weighting: **20%**

This is an individual assignment, the details of which will be posted on iLearn in week 1.

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards

Quiz 3

Due: **31/10/2017**
Weighting: **10%**

The short essay quiz has a time limit of 30 minutes and is conducted online using iLearn. It will cover the material in lectures from weeks 1-11 inclusive.

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk

- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic configuration errors and basic exposures; assess hacking/ hardening techniques and their suitability as controls

Industry presentation

Due: **7/11/2017**
Weighting: **30%**

Presentation to industry experts!

On successful completion you will be able to:

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic configuration errors and basic exposures; assess hacking/ hardening techniques and their suitability as controls

Delivery and Resources

This unit does not rely on any particular technology. However, there is a lot of reading and lab work to be undertaken, this may be don on-campus or off-campus.

Students may find that using their own devices capable of accessing the internet and for reading PDFs whilst off-campus may assist in their group activities.

Unit Schedule

Week/ Date/ Lecturer	Lecture Topic	Reading material

Week 1	Introduction and Course Outline • What is information security? • Comparison between perfect security, technical security and commercial security • Discussion of risk, threat, likelihood and other terminology • Hacking, black hat, white hat, grey hat • Introduction of students, background of education/work experience • Course outline and expectations for deliverables	Senior Executives Commitment to Information Security - from Motivation to Responsibility
Week 2	Standards & Governance • Discussion of different standards and frameworks that they will come into contact with, including ISO27001, ISO27002, Sarbanes-Oxley, PCIDSS, ASIC, COBIT, ITIL • Detailed review of ISO27001 and ISO27002 • Detailed review of SOX and FSRA requirements	ISO/IEC27001, ISO/IEC27002, PCIDSS, Sarbanes Oxley Act, COBIT
Week 3	Information Risk Management Concepts • What is risk • How can it be measured • How is it mitigated • What should be protected • Introduction to information assets • The role of an Information Security Officer • How is risk managed in different industries • Can risks be accepted, should a business be risk-averse	ISO/IEC27005 and ISO/IEC31000, A Novel Security Risk Evaluation for Information Systems, Measuring the risk based value of IT Security solutions, Quantitative assessment of enterprise security system
Week 4	Threat Workshop • What are threats • How are threats measured • Relationship between threats and likelihood • Force Majeure, avoidable threats and how a business reacts to each • Industry specific threats • Technology specific threats • Is privacy a threat?	ISO/IEC27005 and ISO/IEC31000, A Novel Security Risk Evaluation for Information Systems, BSI Handbook, Security Usability Principles for Vulnerability Analysis and Risk Assessment
Week 5	Controls Workshop • What are controls • Understanding the relationship between threats, likelihood and controls • Can controls reduce threats	ISO/IEC27005 and ISO/IEC31000, A Novel Security Risk Evaluation for Information Systems, BSI Handbook

Week 6	Business Continuity Planning and DRP • BCP and DRP overview • Why do it • What can go wrong • BCP/DRP development process and linkage with TRA	ISO/IEC27001, ISO/IEC27005 and ISO/IEC31000, BSI Handbook
Week 7	Creating an Enterprise Information Security Framework • What is an EISF • How are they assessed (ISO/IEC27001, ITIL, COBIT etc) • Importance of scope and statement of applicability • Plan, Do, Check, Act cycle • Evidence, evidence, evidence • What is an Information Security Management System	
Week 8	Information Classification and Exposures • What is information classification • How to classify information • Policies and procedures • Perils of over or under classifying information • Information exposures	ISO/IEC27001, Senior Executives Commitment to Information Security - from Motivation to Responsibility
Week 9	Practical Hacking • History of hacking, why hack an environment • What colour hat do you have • Operating systems and application basics • Tools and techniques	Open Source Security Testing Methodology Manual
Week 10	Incident Response & Server Hardening • Definition of hardening • Operating system basics • Network basics • Application basics • Procedures……more procedures……..and more procedures…..	ISO/IEC27001, Combining ITIL, COBIT and ISO/IEC27002 in Order to Design a Comprehensive IT Framework in Organisations
Week 11	Evidence Collection • Forensics basics • How to collect • What to collect • Roles and responsibilities • When is it better to leave it alone	HB171 Guidelines for the management of evidence, Computer Forensics for Lawyers
Week 12	Physical Security Reviews	

Week 13	Industry presentation

Learning and Teaching Activities

Lectures

Weekly lectures

Labs

Weekly lab work, done in a group representing an operating company or organisation

Assignment

Research assignment into a specific area of information security management

Quizzes

Online quizzes in weeks 4, 8 and 12

Industry presentation

Group presentation to external industry experts for formal assessment

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central. Students should be aware of the following policies in particular with regard to Learning and Teaching:

Academic Honesty Policy http://mq.edu.au/policy/docs/academic_honesty/policy.html

Assessment Policy http://mq.edu.au/policy/docs/assessment/policy_2016.html

Grade Appeal Policy http://mq.edu.au/policy/docs/gradeappeal/policy.html

Complaint Management Procedure for Students and Members of the Public http://www.mq.edu.au/policy/docs/complaint_management/procedure.html

Disruption to Studies Policy (in effect until Dec 4th, 2017): http://www.mq.edu.au/policy/docs/disruption_studies/policy.html

Special Consideration Policy (in effect from Dec 4th, 2017): https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policies/special-consideration

In addition, a number of other policies can be found in the Learning and Teaching Category of Policy Central.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/support/student_conduct/

Results

Results shown in *iLearn*, or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au.

Assessment policy

If you cannot complete a piece of work please see the convenor **before** the due date. Check also the special consideration policy. A more detailed description of each task is given below.

Assessment tasks explained

As the table under assessment tasks indicates, there will be 6 assessment tasks.

- Three online quizzes, the first one is a diagnostic quiz.
- One main individual assignment.
- One group document comprising your lab work from weeks 2-7 inclusive - marked individually.
- A presentation (in week 13) to external industry experts on the work undertaken in labs from weeks 2-11 inclusive. Attendance at the presentation is compulsory.

Your final grade will depend on your performance in each part separately. In particular, to pass this unit you must achieve an overall score of 50%, and achieve at least 40% in the quizzes.

Failure to appear at the industry presentation (without a very good reason) will count as a score of 0 for that component.

All assignments should be handed in via the online system at http://learn.mq.edu.au/ by the time specified in the assignment description.

All work submitted should be readable and well presented.

Late work will be accepted with a penalty of 10% of the marks for the assignment per day submitted late. Hence, an assignment submitted five days late will get at most half the marks. If you cannot submit on time because of illness or other circumstances, please contact the lecturer **before** the due date.

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to improve your marks and take control of your study.

- Workshops

- StudyWise
- Academic Integrity Module for Students
- Ask a Learning Adviser

Student Services and Support

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

IT Help

For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.

Graduate Capabilities

PG - Capable of Professional and Personal Judgment and Initiative

Our postgraduates will demonstrate a high standard of discernment and common sense in their professional and personal judgment. They will have the ability to make informed choices and decisions that reflect both the nature of their professional work and their personal perspectives.

This graduate capability is supported by:

Learning outcomes

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic configuration errors and basic exposures; assess hacking/hardening techniques and their suitability as controls

Assessment task

- Industry presentation

Learning and teaching activity

- Group presentation to external industry experts for formal assessment

PG - Discipline Knowledge and Skills

Our postgraduates will be able to demonstrate a significantly enhanced depth and breadth of knowledge, scholarly understanding, and specific subject content knowledge in their chosen fields.

This graduate capability is supported by:

Learning outcomes

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic configuration errors and basic exposures; assess hacking/ hardening techniques and their suitability as controls

Assessment tasks

- Quiz 1
- Lab work review
- Quiz 2
- Assignment
- Quiz 3
- Industry presentation

Learning and teaching activities

- Weekly lectures
- Online quizzes in weeks 4, 8 and 12
- Group presentation to external industry experts for formal assessment

PG - Critical, Analytical and Integrative Thinking

Our postgraduates will be capable of utilising and reflecting on prior knowledge and experience, of applying higher level critical thinking skills, and of integrating and synthesising learning and knowledge from a range of sources and environments. A characteristic of this form of thinking is the generation of new, professionally oriented knowledge through personal or group-based critique of practice and theory.

This graduate capability is supported by:

Learning outcomes

- Describe and demonstrate how to manage commercial risk, and unmitigated and

mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic configuration errors and basic exposures; assess hacking/ hardening techniques and their suitability as controls

Assessment tasks

- Quiz 1
- Lab work review
- Quiz 2
- Assignment
- Quiz 3
- Industry presentation

Learning and teaching activities

- Weekly lab work, done in a group representing an operating company or organisation
- Research assignment into a specific area of information security management
- Online quizzes in weeks 4, 8 and 12

PG - Research and Problem Solving Capability

Our postgraduates will be capable of systematic enquiry; able to use research skills to create new knowledge that can be applied to real world issues, or contribute to a field of study or practice to enhance society. They will be capable of creative questioning, problem finding and problem solving.

This graduate capability is supported by:

Learning outcomes

- Describe and explain the differences between security frameworks and standards
- Describe and demonstrate how to manage commercial risk, and unmitigated and mitigated risk
- Identify and assess commercial threats and types of threats and statutory requirements in a commercial environment
- Identify and analyse basic configuration errors and basic exposures; assess hacking/ hardening techniques and their suitability as controls

Assessment tasks

- Lab work review
- Quiz 2

- Assignment
- Industry presentation

Learning and teaching activities

- Weekly lab work, done in a group representing an operating company or organisation
- Research assignment into a specific area of information security management

PG - Effective Communication

Our postgraduates will be able to communicate effectively and convey their views to different social, cultural, and professional audiences. They will be able to use a variety of technologically supported media to communicate with empathy using a range of written, spoken or visual formats.

This graduate capability is supported by:

Learning outcome

- Describe and explain the differences between security frameworks and standards

Assessment tasks

- Lab work review
- Quiz 2
- Assignment
- Industry presentation

Learning and teaching activities

- Weekly lab work, done in a group representing an operating company or organisation
- Research assignment into a specific area of information security management
- Group presentation to external industry experts for formal assessment

PG - Engaged and Responsible, Active and Ethical Citizens

Our postgraduates will be ethically aware and capable of confident transformative action in relation to their professional responsibilities and the wider community. They will have a sense of connectedness with others and country and have a sense of mutual obligation. They will be able to appreciate the impact of their professional roles for social justice and inclusion related to national and global issues

This graduate capability is supported by:

Learning outcome

- Describe and explain the differences between security frameworks and standards

Learning and teaching activities

- Weekly lectures
- Group presentation to external industry experts for formal assessment

Standards

Standards

Four standards, namely HD, D, CR, P summarise as many different levels of achievement. Each standard is precisely defined to help students know what kind of performance is expected to deserve a certain mark.

Grade	LO 1	LO 2	LO 3	LO 4
	Architectures	Risks	Threats	Controls
HD	Detailed understanding of the differences between architectures, standards, legislation and industry regulations. Can apply the correct architecture to meet different requirements. Can manage the design and implementation process of a project to use one of the architectures.	Detailed understanding of information security risks and risk management. Can demonstrate the correct approach to risk identification and information gathering. Can produce a correct Risk Register and Risk Treatment Plan. Can demonstrate a sound understanding of personnel related information security risk processes. Can produce a detailed BIA and understand management response to risk.	Detailed understanding of threats, threat vectors, likelihood an impact. Can manage complex scenario-based information gathering to produce a business-oriented threat matrix. Can demonstrate the selection process for metrics and identify novel approaches to selection in complex scenarios.	Can demonstrate and manage a process to identify and select appropriate controls. Can demonstrate an understanding of the different classes of controls, their limitations and how to choose and implement the most appropriate controls.
D	Some understanding of the differences between architectures, standards, legislation and industry regulations. Can identify the correct architecture to meet different requirements. Can create the design and implementation process of a project to use one of the architectures.	Some understanding of information security risks and risk management. Can demonstrate the correct approach to risk identification and information gathering with assistance. Can produce either a correct Risk Register or a correct Risk Treatment Plan. Can demonstrate a sound understanding of personnel related information security risk processes. Can produce a partial BIA and understand management response to risk.	Some understanding of threats, threat vectors, likelihood an impact. Can manage simple scenario-based information gathering to produce a business-oriented threat matrix. Can demonstrate the selection process for metrics.	Can demonstrate and manage a process to identify and select appropriate controls. Can demonstrate an understanding of most of the different classes of controls, their limitations and how to choose and implement the most appropriate controls

CR	Some understanding of the differences between architectures, standards, legislation and industry regulations. Can identify the correct architecture to meet different requirements. Can manage the design and implementation process of a project to use one of the architectures.	Some understanding of information security risks and risk management. Can demonstrate the correct approach to risk identification and information gathering with assistance. Can produce a partial Risk Register and a partial Risk Treatment Plan. Can demonstrate some understanding of personnel related information security risk processes. Can produce a partial BIA or demonstrate the principles behind management response to risk.	Some understanding of threats, threat vectors, likelihood an impact. With assistance, can manage simple scenario-based information gathering to produce a business-oriented threat matrix. With assistance, can demonstrate the selection process for metrics.	Can explain processes to identify and select appropriate controls. Can demonstrate an understanding of the different classes of controls, their limitations and how to choose and implement the most appropriate controls
P	Some understanding of the differences between architectures, standards, legislation and industry regulations. May not always apply the correct architecture to meet different requirements. Cannot identify the design and implementation process of a project to use one of the architectures without assistance.	Some understanding of information security risks and risk management. Can demonstrate the correct approach to risk identification and information gathering with assistance. Can produce a partial Risk Register and a partial Risk Treatment Plan with assistance. Can demonstrate some understanding of personnel related information security risk processes. With assistance, can produce a partial BIA or demonstrate the principles behind management response to risk.	Some understanding of threats, threat vectors, likelihood an impact. With assistance, can explain simple scenario-based information gathering to produce a business-oriented threat matrix. With assistance, can explain the selection process for metrics.	With assistance, can explain processes to identify and select appropriate controls. With assistance, can explain some of the different classes of controls and their limitations.

Grading

At the end of the semester, you will receive a grade that reflects your achievement in the unit

- **Fail (F)**: does not provide evidence of attainment of all learning outcomes. There is missing or partial or superficial or faulty understanding and application of the fundamental concepts in the field of study; and incomplete, confusing or lacking communication of ideas in ways that give little attention to the conventions of the discipline.
- **Pass (P)**: provides sufficient evidence of the achievement of learning outcomes. There is demonstration of understanding and application of fundamental concepts of the field of study; and communication of information and ideas adequately in terms of the conventions of the discipline. The learning attainment is considered satisfactory or adequate or competent or capable in relation to the specified outcomes.
- **Credit (Cr)**: provides evidence of learning that goes beyond replication of content knowledge or skills relevant to the learning outcomes. There is demonstration of substantial understanding of fundamental concepts in the field of study and the ability to apply these concepts in a variety of contexts; plus communication of ideas fluently and clearly in terms of the conventions of the discipline.
- **Distinction (D)**: provides evidence of integration and evaluation of critical ideas, principles and theories, distinctive insight and ability in applying relevant skills and

concepts in relation to learning outcomes. There is demonstration of frequent originality in defining and analysing issues or problems and providing solutions; and the use of means of communication appropriate to the discipline and the audience.

- **High Distinction (HD)**: provides consistent evidence of deep and critical understanding in relation to the learning outcomes. There is substantial originality and insight in identifying, generating and communicating competing arguments, perspectives or problem solving approaches; critical evaluation of problems, their solutions and their implications; creativity in application.

In this unit, your final grade depends on your performance in each part of the assessment. For each task, you receive a mark that combines your standard of performance regarding each learning outcome assessed by this task. Then the different component marks are added up to determine your total mark out of 100. Your grade then depends on this total mark and your overall standards of performance.

Your final grade will depend on your performance in each part separately. In particular, to pass this unit you must achieve an overall score of 50%, and achieve at least 40% in the quizzes.

Failure to appear at the industry presentation (without a very good reason) will count as a score of 0 for that component.

Obtaining a grade higher than a Pass (P) in this unit will require a student to obtain (in addition to the above):

- the required total number of marks (Credit - 65, Distinction - 75, High Distinction - 85).