TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

School of Information Management

MMIM 581

SECURITY AND RISK IN INFORMATION MANAGEMENT

Trimester 2 2012

COURSE OUTLINE

Contact Details	
Course Coordinator:	**Jeremy McKissack** **Room: RH 419** **Phone: 463 5233 extn 7436** **Email: jeremy.mckissack@vuw.ac.nz**
Programme Administrator:	**Usha Varatharaju** RH 521, Level 5, Rutherford House, Wellington Ph:- (054) 463 5309 e-mail :- usha.varatharaju@vuw.ac.nz
Dates:	**16th July to 19th October 2012**
Times:	**Time: Tuesday 5.40pm – 7.30pm**
Venue:	**Room: RHG02**

Course Objectives:

Security and risk have become crucial to the management and use of information and information systems. Issues include an understanding of the risks associated with information systems security, why they are a matter for concern across all levels of the organisation, how risk and security assessments should be done in terms of impact on systems integrity, impact on systems, impact on staff, impact on reputation and on market share.

More specifically stated the course objectives are to:

1. Help students understand and appreciate information security threats, vulnerabilities and impacts arising from the use of information systems to support business processes.
2. Consider the implications of system and network vulnerability in the context of business strategy, strategic risk management and IT governance.

3. Provide a conceptual management framework with which to address information security risks in a coherent and structured manner (*e.g*. how to assess the suitability of security controls proposed for a new business IT system; how to balance potential security impacts against the costs of control).
4. Relate theory to practice through the use of case studies and classroom discussion based on real world experience of information security management.

Note that this is not a course in the technology of information systems security. It is a management course intended to sensitize students to security and risk issues that impact on management considerations in an information age.

Learning Outcomes:

By the end of this course students should be able to:

1. Undertake library and internet research and record their findings according to standard academic requirements.
2. Understand some of the important philosophical, technical and commercial principles underpinning information security risks, practices and controls.
3. Evaluate the business opportunities and limitations that information security risk place upon managers.
4. Appreciate the use of information security within an organisation's risk management practice and general governance framework.
5. Discuss intelligently information security risk and control issues in Information Management.

Withdrawal from Course

1. Your fees will be refunded if you withdraw from this course on or before Friday 27 July 2012.

2. The standard last date for withdrawal from this course is Friday 28 September 2012. After this date, students forced to withdraw by circumstances beyond their control must apply for permission on an '*Application for Associate Dean's Permission to Withdraw Late'* including supporting documentation. The application form is available from either of the Faculty's Student Customer Service Desks.

Course Delivery

The course will be delivered in seminar form with in class discussions, group work as well as lectures. Modules will more or less equate to lectures, depending on progress made each week.

There will be no course examination, but there will be a 90 minute written case study test during the final class.

Date	Topic	Readings
17th July	Course administration and general introduction to the course.	None
24th July	The information security problem and security models.	Chapter 3: Legal, Ethical and Professional Issues. Chapter 5: (section) Policy, Standards and Practices

31st July	Risk management QRA Exercise	Chapter 4: Risk Management
7th August	Protecting information systems.	Chapter 2: The need for security Chapter 9: Physical security
14th August	Network security controls	Chapter 6: Security Technology Chapter 7: (section) Intrusion Detection
21st August	Identity management and user administration	Chapter 7: (section) Access Control Devices Chapter 11:Security and Personnel
11th September	Group project 1: Present risk management plan to class. Incident response processes and issues arising	Chapter 5: (section) Continuity Strategies
18th September	New technology, threats and business innovation.	Chapter 8: Cryptography
25th September	Security metrics, monitoring and reporting.	
2nd October	Investment decisions for information security. Introduce final case study.	Chapter 10: Implementing Information Security Chapter 12: Information Security Maintenance
9th October	Group project 2: present system security plan to class. Recap, sum up and feedback.	
16th October	Final class case study/test.	All

Readings

Extensive use will also be made of the Internet to obtain current material. Student assignments will also be prepared from information available in the library and on the Internet, but care should be taken to ensure that only authoritative sources are used. Because the topics dealt with change so fast, where appropriate, reading lists and papers will be handed out to students. Use will also be made of the teaching and communications potential available through Blackboard software on the VUW website. Students are advised to subscribe to Crypto-gram at www.counterpane.com

Students will be required to prepare for classes by reading, in advance, relevant chapters of Whitman, M. E. & Mattord, H. J. (2005) *Principles of Information Security,* 3rd ed. Boston, Ma.: Thomson Course Technology. (ISBN 9781435488847). This book will be available from VicBooks on the Pipitea campus. Students should also be able to discuss intelligently any of the questions at the end of each chapter prepared for that lecture.

In addition, the following books will be useful for students studying this course:-

Panko, R. R. (2005) *Business data networks and telecommunications.* 5th ed. Upper Saddle River, N.J.; Pearson/Prentice Hall.

Winkler, I. (2005) *Spies Among Us.* Wiley. ISBN 0-7645-8468-5

M. Gentile, R. Collette and T. August (2006) *The CISO Handbook - a practical guide to securing your company* Auerbach. ISBN: 0-8493-1952-8

New Zealand Information Security Manual (2010), [online]
http://www.gcsb.govt.nz/newsroom/nzism/NZISM_2011_Version_1.01.pdf

Course website:

Full course details and course materials are, or will be, available on Blackboard at:

http://blackboard.vuw.ac.nz

Please check the web site regularly.

Assessment:

Most sessions will commence with a short presentation, by two students, of their preparation assignments. These assignments are based on readings and exercises from Whitman and Mattord. The purpose of these assignments, and subsequent discussions, is to get students thinking about the subject area in a typical business context.

- Group projects oral & written 25%
- Session Preparation Assignments (6) 40%
- Final in-class case study 35%

Quality Assurance Note

Your assessed work may also be used for quality assurance purposes, such as to assess the level of achievement of learning objectives as required for accreditation and audit purposes. The findings may be used to inform changes aimed at improving the quality of FCom programmes. All material used for such processes will be treated as confidential, and the outcome will not affect your grade for the course.

Expected Workload

Assessment item	Date Due	For detailed instructions see	%age of total grade	Expected time allocation
Session Preparation Assignments - SPAs	According to schedule	Appendix 1	40	60 hours
Group Project: 1 Risk Management Plan	11 Sept. 2012	Appendix 2	10	25 hours
Group Project: 2 System Security Plan	9 Oct. 2012	Appendix 2	15	45 hours
Case study / Test	16 Oct. 2012	Appendix 3	35	20 hours
Total			100	150 hours

Group Work

Refer to Appendix 2

Materials and Equipment

It is expected that students will have ready access to a personal computer as well as Internet access. This will be necessary for receiving and sending course-related email, for accessing the course web site on Blackboard, and for other similar purposes.

Grading standards:

Letter Grade	Number grade	Approx Dist'n *	Simple Description	More Complete Description**
A+	Over 84	4%	Outstanding	Far exceeds requirements, flawless, creative
A	80-84	10%	Excellent	Polished, original, demonstrating mastery
A-	75-79	14%	Very Good	Some originality, exceeds all requirements
B+	70-74	22%	Good	Exceeds requirements in some respects
B	65-69	26%	Satisfactory	Fulfills requirements in general
B-	60-64	18%	Acceptable	Only minor flaws. Unoriginal
C+	55-59	4%	Pass	Mistakes, recapitulation of course material
C	50-54	2%	Minimum pass	Serious mistakes or deficiencies
D	40-49	1%	Unacceptable	Little understanding, poor performance
E	00-39	1%	Fail	Below the minimum required

* This is the hypothetical percentage of students that would attain the various levels of performance, over several repetitions of the course, under similar conditions. It is recognised that the distribution in a particular course, particularly with small enrolment, may differ markedly from the long-term distribution.

** The lecturer will develop a more complete or specific description of the meaning of the various levels of performance based upon the specific nature of the assessment in a course. For example, performance may be determined by the qualities of a written report, a classroom presentation, or work in a group project. The words sued to describe these kinds of assessments will obviously vary.

Format of Assignments:

Assignments must be submitted in hard copy to the paper Coordinator. They should be computer-formatted, 12pt font, 1.5 line spacing, single sided papers, to allow for written comments on the paper. Length of the document should be between 10 to 15 pages. Appendix material does not count toward the required assignment length. Where appropriate, use should be made of the APA bibliographic convention available from http://general.rau.ac.za/library/bibweb/html/index.htm

Penalties for Lateness & Excessive length

In keeping with standards of professionalism appropriate to this programme, it is expected that deadlines will be honoured. In fairness to students who complete work on time, work submitted after the due date/ time will incur penalties for lateness. The penalty is up to 5 % of the report's grade per day (or part thereof) late. Unusual or unforeseeable circumstances (*e.g*. serious illness, family bereavement) may lead to a waiver of this penalty but need to be discussed with the paper coordinator as soon as possible. Being succinct and staying focused is an important management skill so excessively long assignments will be penalized *pro rata* according to the extent of overrun (*e.g*. 25% score reduction for a paper that is 125% of the stated maximum length).

Class Representative

A class representative will be elected in the first class, and that person's name and contact details made available to VUWSA, the Course Coordinator and the class. The class representative provides a communication channel to liaise with the Course Coordinator on behalf of students.

Communication of Additional Information
Additional information or information on changes will be conveyed to students via Blackboard.

Use of Turnitin

Student work provided for assessment in this course may be checked for academic integrity by the electronic search engine http://www.turnitin.com Turnitin is an on-line plagiarism prevention tool which compares submitted work with a very large database of existing material. At the discretion of the Head of School, handwritten work may be copy-typed by the School and subject to checking by Turnitin. Turnitin will retain a copy of submitted materials on behalf of the University for detection of future plagiarism, but access to the full text of submissions will not be made available to any other party.

For the following important information follow the links provided:

Academic Integrity and Plagiarism
http://www.victoria.ac.nz/home/study/plagiarism.aspx

General University Policies and Statutes
Find key dates, explanations of grades and other useful information at
www.victoria.ac.nz/home/study
Find out about academic progress and restricted enrolment at
http://www.victoria.ac.nz/home/study/academic-progress.aspx
The University's statutes and policies are available at www.victoria.ac.nz/home/about/policy, except qualification statutes, which are available via the Calendar webpage at
http://www.victoria.ac.nz/home/study/calendar.aspx (See Section C).
Further information about the University's academic processes can be found on the website of the Assistant Vice-Chancellor (Academic) at
www.victoria.ac.nz/home/about_victoria/avcacademic/default.aspx

AVC (Academic) Website: information including: Conduct, Academic Grievances, Students with Impairments, Student Support
http://www.victoria.ac.nz/home/about_victoria/avcacademic/Publications.aspx

Faculty of Commerce Office
http://www.victoria.ac.nz/fcom/studenthelp/

Te Putahi Atawhai
Maori and Pacific Mentoring Programme
http://www.victoria.ac.nz/tpa/

Appendix 1

MMIM 581 – Security and Risk in Information Management

Assessment 1 - Session Preparation Assignments - SPAs

There will be six Session Preparation Assignments – SPAs – during the course. The readings for each SPA will be posted to the BlackBoard website. Students will be expected to read the document and come to class prepared to discuss the issues presented. These SPAs are designed to give students practice with the analysis of texts and the identification of issues of relevance to lectures and class discussions. As such they prepare students for the end-of-term case study test. Contribution to each class will be assessed and the mark awarded will contribute to the final grade.
Learning outcomes: 1, 2 and 4.

Appendix 2

MMIM 581 – Security and Risk in Information Management

Assessment 2 – Group projects

A recurrent theme running through the lectures will be the security and risk considerations that various organisations would experience. The primary objective of this assignment is to provide students with an opportunity to pull together and organise material concerning information security in a form that is understandable to a senior manager, and effectively present that material to an executive-level team.

To facilitate the group project students will be asked, during session 1, to form three groups each taking the role of a new security team within one of three organisations. Each of these three organisations will be associated with a different industry sector (finance, government or e-business). Group projects throughout the course will encourage discussion of the material as it might relate differently to each of the organisations.

Using a template to be handed out and discussed in class, the plans will build on material dealt with in class.

Project 1
A class presentation will be made during Session 7. Each group will present a proposal for a risk management plan for their organisation. Backing this up, each group will submit an 8 page written report with their oral presentation and will answer any questions from the class. The report should include references to the organisations business environment, objectives, business processes and technologies. The written submission will contribute to the course mark of each student, both on a group basis and on an individual basis – according to the assessment ratio given below.

Project 1 will be assessed based on the written submissions (10%).

Project 2
During session 11 a presentation will be made to the class acting as the "Senior Leadership Team" of their organisation. Each group will make an oral presentation identifying the process by which the system security plan will be implemented and monitored. Backing this up, each

group will submit an 8 page written report with their oral presentation and will answer any questions from the "Senior Leadership Team". The report should include references to the risk management plan, the organisations business goals and strategy and its business processes and technologies. The written submission will contribute to the course mark of each student, both on a group basis and on an individual basis – according to the assessment ratio given below.

Learning outcomes: 1, 2 and 3.\
Project 2 will be assessed based on the oral presentation (5%) and the written submission (10%).

Structure of assignment

The standard structure of the written assignment (10%) will be:-

- Title Page
- A business summary of about one page summarizing the document's main points and findings. This is usually written right at the very end, when the assignment is completed. It serves to summarize the contents and findings of the document so that a potential reader can decide whether to read the full document or not.
- Using a template to be handed out and discussed in class, the report will build on material dealt with in class, but applied to their organisation.
- Appendices will give technical or evidential detail to support the arguments of the text. Material would be placed in this section to prevent detail from interfering with the logical flow of the written proposals.
- The written assignment should be about 10 pages in length, twelve point Times New Roman type font and with 1.5 line spacing, with a left-hand margin, unjustified.

Oral Assignment
The oral component of the assignment requires the team to "sell" the plan to senior leadership. The team will be awarded up to 5% of the course mark based on the content and delivery of their presentation.

Appendix 3

MMIM 581 – Security and Risk in Information Management

Case Study Test

The open-book class test at the end of the course is designed specifically to assess how students have assimilated material dealt with in class and in other assignments and what they make of that material. Rather than assessing memory, these tests are intended to assess student thinking and understanding. The ability to communicate that understanding therefore becomes a critical success factor.

In preparation for the class exercise, students will be required to read a case study to be handed out in class in week 11. Particular attention should be paid to the following:-

- The security and risk issues emerging from the case;
- How these relate to the principles addressed in class discussions;
- What you think would be the best approach to resolving the problems or issues identified.

Please note that during the MMIM 581 class on Tuesday 16th October 2012 a questionnaire will be handed out with an answer book. Students will be required to answer 5 of the 8 questions set and hand back the answer book before leaving the class. Full instructions will be given with the questionnaire. The time limit will be 90 minutes. Students may bring into the class any books or reference materials they may require. It is recommended that careful consideration be given to the resources brought into class. Experience reveals that too many resources are time consuming and burdensome to work with in a test of this length and nature.

Of particular importance to note is that this case study exercise is part of "Terms" and students must obtain a minimum mark of 45% in order to pass the MMIM 581 course. The mark obtained contributes 35% of the final overall course mark.

Learning outcomes: 2 and 4.