VICTORIA UNIVERSITY OF WELLINGTON
Te Whare Wananga o te Upoko o te Ika a Maui

Faculty of Commerce and Administration

School of Information Management

MMIM 581

SECURITY AND RISK IN INFORMATION MANAGEMENT

Contact Details	
Paper Coordinator:	**Tony Hooper** Easterfield Building, Kelburn Parade Wellington Ph:- 463 5015 Email: tony.hooper@vuw.ac.nz
Programme Administrator:	**Ruth Neethling** Easterfield Building, Kelburn Parade, Wellington Ph:- 463 5309 e-mail :- Ruth.Neethling@vuw.ac.nz
Lecturers	**Rupert Dodds –KPMG Wellington - (04) 816 4521** **Email – rdodds@kpmg.co.nz** **Alin Ungureanu – KPMG Wellington – (04) 816 4882** **Email – alinu@kpmg.co.nz**
Dates:	**28th February 2007 to 28th May 2007**
Times:	**Thursday 5.40pm – 7.30pm**
Venue:	**RLWY 128**

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:

- Undertake library and Internet research and record their findings according to standard academic requirements.
- Understand some of the important philosophical, technical and commercial principles underpinning information security risks and controls.
- Evaluate the business opportunities and limitations that information security risk place upon managers.
- Appreciate the use of information security as a risk management tool, the alignment of both, and how they contribute to the organization's general governance framework.
- Discuss intelligently information security risk and control issues in Information Management - what they are, what makes them important, damage control and how incidents should be handled, and what the consequences of breaches can be for managers in business and government.

Paper Content and schedule:

Modules will more or less equate to lectures, depending on progress made each week:

1. Course administration and general introduction to course
2. Information security, risk and control. Evaluating security risks to derive security control requirements
3. Network perimeter security controls
4. Internal network security controls
5. Identity management and user administration
6. Physical security controls; discuss group project
7. Incident response processes and issues arising
8. Systems resilience and disaster recovery for business continuity
9. Security metrics, monitoring and reporting
10. Investment decisions re information security; introduce final project
11. In class group project presentation. Recap, sum up and feedback
12. Final class case study.

Paper Resource Materials:

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 chapters of Whitman, M. E. & Mattord, H. J. (2005) *Principles of Information Security,* 2nd ed. Boston, Ma.: Thomson Course Technology. (ISBN 0-619-21625-5) This book will be available from VicBooks on the Pipitea campus.

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

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.

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.

Course project:

1. Group project (Delivery dates to be determined once groups have been identified)

Students in groups of three or four during Session 4 or 5, will present a risk identification and control design for a selected business, based on information obtained from lectures. Each group will carry out a preliminary analysis on interview data to identify the main risks, then perform a quantitative risk analysis (based on a very limited, simplified formula) on those risks, and prioritise the risks accordingly. The group will then suggest and justify controls to reduce the significant risks. Groups do not need to get too much into the technological aspects. The cost-justification is a fairly basic approach but the aim is to stimulate the thinking rather than to "get it right".

A final class presentation will be made to the “Board of Directors” during Session 11. Each group will make an oral presentation identifying the process by which the security policy will be implemented and monitored. In addition, each group will submit a written report with their oral

presentation and will answer any questions from members of the Board. The written report should include a critical reflection on the risk-based techniques employed by the group and any other interesting aspect of the investigation. 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. Details will be made in class as soon as the demographic details of the class are known.

2. Individual written project. (Delivery date Thursday 12th April 2007 in class or by email before midnight.)

A recurrent theme running through the lectures will be the security and risk considerations that TradeMe would experience. Reference will be made in lectures to TradeMe and the company will be used as an example to illustrate aspects of Information Security and Risk Management. From the view point of the Fairfax Acquisition Team each student will prepare a written report to the Fairfax Board on their "due diligence" from the technology perspective on the TradeMe acquisition, identifying the particular problems the topic presents. The primary objective of this assignment is to provide students with an opportunity to practice presenting a business report to management.

Structure of assignment

The standard structure of the written assignment 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 TradeMe as a business.
- The final part of the submission must include how the "due diligence" will be discharged in the case of the TradeMe acquisition.
- 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.

Assessment:

Most sessions will commence with a short case study relevant to the session. There will be no specific preparation required: the idea is to stimulate discussion and get students thinking about the subject area in a typical business context.

- Group project written 30%

- Individual project (written component) 40%
- Final in-class case study 30%

Terms:

- Completion of group and individual written projects on time and in format required
- Scoring at least 45% for the final in-class case study.
- Attending at least 75% of classes.

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).

General University Requirements:

Students should familarise themselves with the University's requirements, particularly those regarding assessment and course of study requirements, and formal academic grievance procedures, contained in the Statutes of the Calendar and read the requirements of this paper outline in that context. The Statute on Conduct ensures that members of the University community are able to work, learn and study and participate in the academic and social aspects of the University's life in an atmosphere of safety and respect. The Statute contains information on what conduct is prohibited and what steps can be taken if there is a complaint.

The Statute on Conduct is published on the University's website (http://www.vuw.ac.nz/publications/calendar) or may be viewed at the Reserve Book Room in the University Library.

Grievances:

If you have any academic problems with your paper, you should talk to the lecturer concerned or, if you are not satisfied with the result of that meeting, see the Head of School, or the Associate Dean (Students) of your Faculty.

Plagiarism:

Plagiarism is not acceptable in any form. Plagiarism takes many forms and includes:

- deliberately copying another student's work,
- copying directly from text books and other sources without using quotations marks,
- not acknowledging the sources you have used in your work (*i.e.* you must cite all references),
- re-submitting an assignment from one course as an original piece of work for another.

Work that shows evidence of plagiarism will be penalized in line with the seriousness of the case. This may involve work being returned unmarked, and consequent failure of the course. In extreme cases, University academic disciplinary procedures may be invoked.