BUSINESS SCHOOL

Course Outline 2019

INFOSYS 727: ADVANCED INFORMATION SECURITY (15 POINTS)

Semester 1, (1193)

Course prescription

Focusses on technical security issues of the system used in today's information technology applications. Explores the practical issues of identification and authentication, security of operating systems, cryptography, disaster recovery and contingency planning, and discusses the relevant theoretical models. Managerial aspects of information security issues as well as legal and ethical issues arising from protecting computer files both in New Zealand and global perspective will be addressed. The course follows the content of CISSP certification.

Course advice

There is no specific prerequisites required to have to be enrolled in this course but sound knowledge of IT hardware and software would significantly help to deal with the course content.

Goals of the course

This course presents technical and organisational arrangements of making information systems more secure. This process starts with defining the proper approach to setting up a security system, which are culminates with development of security policy. Basic components of security system will be discussed: firewalls, intrusion detection systems, encryption, security assessment, and security standards. Typical defences against viruses and other malicious software will be presented. Phenomena of cyber terrorism and cyber warfare will also be covered.

This course is a next logical step after gaining basic knowledge related to use of information systems in business. After graduation from this course the students will be able to effectively use their information technology tool without fear of being exposed to possible attacks against their IT systems.

This course is a preparatory step for studying toward obtaining the Certified Information Systems Security Professional (CISP), being the world most known information security professional certification.

The course will provide students with advanced disciplinary knowledge and practice in the field of information security, allows them to critically and independently evaluate related to that field knowledge and provide adequate solution to a problem.

Learning outcomes (LO)

By the end of the course, it is expected that students will be able to:

#	Learning outcome	Graduate profile capability*
LO1	Shows advanced knowledge of the information security concepts (security protocols, human-computer interfaces, access control, cryptography and distributed systems issues)	1. Disciplinary knowledge and practice
LO2	Evaluate and apply solution solving developmental, managerial and audit issues including the review of the related law, evidence collection and security policies	2. Critical thinking
LO3	Demonstrate critical and creative thinking to formulate and justify appropriate recommendations and/or solutions to an information security problem	3. Solution seeking 2. Critical thinking
LO4	Present an argument in highly structured format and clearly discuss the central ideas.	4b. Communication (Written) 2. Critical thinking
LO5	Contribute to own team's success by helping the team to move forward, participating in setting goals, and articulating alternative ways to solve problems	4c. Engagement (Collaboration)

* See the graduate profile this course belongs to at the end of this course outline.

Content outline

Week / Module	Topic	Relevant learning resources/activities	Assessment due this period
1	Course introduction, Basic hardware, software, internet	Handouts	
2	Cryptography	Chapter 5	Class test 1
3	Information Security and Risk Management	Chapter 1	Class test 2
4	Access control	Chapter 2	Class test 3
5	Software Development Security	Chapter 3	Class test 4
6	Business Continuity and Disaster Recovery Planning	Chapter 4	Class test 5
7	Legal, Regulations, Compliance and Investigations Electronic and information warfare	Chapter 6	Class test 6
8	Operations Security	Chapter 7	Class test 7
9	Physical and Environmental Security	Chapter 8	Class test 8

Week / Module	Topic	Relevant learning resources/activities	Assessment due this period
10	Security Architecture and Design	Chapter 9	Class test 9
11	Telecommunication and Network Security	Chapter 10	Class test 10
12	Ten Domains of CISSP Security, Course review	Appendix A	

The module length is approximately one week; each topic is a subject of possible changes.

Security Lab

10 one-hour lab sessions, starting at the second week of the term, subject of possible changes.

Session	Topic
1	Cryptography, part 1
2	Cryptography, part 2
3	Digital forensic
4	Windows security, firewalls
5	1st Lab Test
6	Wireshark, part 1
7	Wireshark, part 2
8	WEB Goat
9	Risk Analysis
10	2nd Lab Test

Learning and teaching

The structure of this course reflects the 10 domains of knowledge for obtaining the CISSP certification (CISSP: Certified Information Systems Security Professional). IT includes such professional practices like access control, cryptography, physical security, related regulations, polices, laws, and other organizational categories.

The course is the first step on the way to get CISSP certification or becoming an information security professional.

This course need about 150 hours learning during the semester including:

- 36 contact hours
- 24 hours preparatory reading
- 90 hours of self-study

The key to successful completion of the course without much stress is a regular study during the whole semester.

Attendance at the lectures is not obligatory but is highly recommended.

Lectures will be recorded.

To encourage communications within the class Piazza system will be activated.

Teaching staff

Course director
A/P Lech J. Janczewski
Office: OGGB Room 480
Tel: 923 7538
Email: lech@auckland.ac.nz

Tutor:
Farzan Kolini
Email: f.kolini@auckland.ac.nz

Learning resources

- Course will follow the textbook: P. Gregory, **CISSP Guide to Security Essentials**, Course Technology, second edition, 2015, ISBN 978-1-285-06042-2

Other useful books:

- M. Whitman and H. Mattord. Principles of Information Security, Thomson - Course Technology, 2014, Fifth Edition
- L. Janczewski, W. Caelli, Cyber Conflicts and Small States, Ashgate, ISBN 978-1-4724-5219-1
- Software used in lab: Provided by Instructor
- Lectures notes distributed via Canvas
- Links to related publications in newspapers, magazines and journals will be provided from time to time**.**

Students are required to complete the prescribed readings and be fully prepared to contribute to the in-depth discussions.

Assessment information

Assessment task	Weight %	Group and/or individual	Submission
8 lab exercises	8	Individual	Immediately after completion of lab session
1st lab test	6	Individual	At the exam time
2nd lab test	6	Individual	At the exam time
Group project	10	Group	Two weeks before the end of lectures
10 class tests	20	Individual	Starting at 2nd week, collected immediately after each test

Assessment task	Weight %	Group and/or individual	Submission
Final examination	50	Individual	At the exam time

Description of assessment tasks

Assessment task	Learning outcome to be assessed
Weekly class test: covers material presented since the previous class quiz. Contain 10 questions with 5 answers of which only one is correct. One minute per question, answers on a special paper form.	LO1, LO2, L03
Lab exercises: Covers content of 8 topics listed above and terminates with a submission of a lab report	LO1, L02
2 Lab tests: Online test covers content of the previous 4 labs	L01, L02, L03
Group project: Distributed at the beginning of the semester. Work in 4 students' teams.	L04, L05
Final examination: Short answers to 30 questions related to the topics presented in the class and lab exercises, lasting 3 hours.	L01, L02, L03, L04

Inclusive learning

Students are urged to discuss privately any impairment-related requirements face-to-face and/or in written form with the courses convenor/lecturer and/or tutor.

Academic integrity

The University of Auckland will not tolerate cheating, or assisting others to cheat, and views cheating in coursework as a serious academic offence. The work that a student submits for grading must be the student's own work, reflecting his or her learning. Where work from other sources is used, it must be properly acknowledged and referenced. This requirement also applies to sources on the worldwide web. A student's assessed work may be reviewed against electronic source material using computerised detection to provide an electronic version of their work for computerised review.

Student feedback

- We regularly seek feedback from students in order to shape and improve this and all courses on the programme.
- Students will be asked to complete:
  - Formative fast feedback early in the semester
  - Course and teaching evaluations at the end of the course
- We will seek volunteers to serve as class reps.

In the event of an unexpected disruption

We undertake to maintain the continuity and standard of teaching and learning in all your courses throughout the year. If there are unexpected disruptions, the University has contingency plans to ensure that access to your course continues and your assessment is fair, and not compromised. Some adjustments may need to be made in emergencies, In the event of a disruption, the University and your course coordinators will make every effort to provide you with up to date information via Canvas and the University website.

Graduate profile for MCom

The following six themes represent the capabilities that the Business School seeks to foster in all of its graduates. The development of these capabilities does not come all at once, but rather is expected to build from year to year. Each course is not expected to contribute to all capabilities, but each course will have its own goals and learning outcomes that relate to the overall development of this profile.

Graduate Profile
1. Disciplinary knowledge and practice Graduates will be able to apply highly specialised knowledge within the discipline to demonstrate an advanced awareness and understanding in a global context.
1. Critical thinking Graduates will be able to analyse and evaluate the relevant literature, and design and develop scholarly arguments that demonstrate advanced and diverse thinking.
2. Solution seeking Graduates will be able to creatively research and analyse complex issues, and develop innovative solutions.
3. Communication and engagement Graduates will be able to engage, communicate, and collaborate with diverse groups using multiple formats and effectively address a range of professional and academic audiences.
4. Independence and integrity Graduates will be able to demonstrate advanced independent thought, self-reflection, ethics, and integrity.
5. Social and environmental responsibility Graduates will consider, in relation to their discipline, the potential significance of the principles underpinning both the Treaty of Waitangi and sustainability.