

Concordia University College of Alberta

Master of Information Systems Security Management Degree

Term Summary (most common sequence for full-time students)

Fall Term (September – December 2006) Faculty

ISSM 543 Systems Development & Project Management	TBA
ISSM 511 Introduction to Information Systems Security	TBA
ISSM 521 TCP/IP Architecture	TBA
ISSM 541 Financial Management & Analysis	TBA
ISSM 553 Risk Management and Analysis	TBA

Winter Term (January to April 2007) Faculty

ISSM 535 Firewall Fundamentals	TBA
ISSM 538 Research Methods I	TBA
ISSM 525 Securing an E-Commerce Infrastructure	TBA
ISSM 507 Organizational Behavior	TBA
ISSM 533 Cryptography & Secure Network Communications	TBA

Spring Term (May to July 2007) Faculty

ISSM 536 Forensics (New)	TBA
ISSM 545 Security Policies, Standards, and Management	TBA
ISSM 531 Advanced Network Security	TBA
ISSM 561 Information Technology Security Laws and Ethics	TBA
ISSM 539 Research Methods 2	TBA
ISSM 551 Disaster Recovery Planning	TBA

Research Project (August to November) Faculty

ISSM 570 Practicum Research Project or ISSM 571 Research Project in Subject Area.
Faculty responsible for this chosen by Management Policy Committee.

Normally students enter the program full-time in the fall and start their research the following August or September. Students are not permitted to register in Research Methods II unless they are projected to successfully have completed all courses and maintain a 3.0 or better average in the program. Research Methods II is required before any Research Project may begin.

Note: Students must complete prerequisites before entering the program.

Course Descriptions

ISSM 507 Organizational Behavior

Organizational behavior integrates content from several fields including psychology, sociology, economics, organization theory, statistics, and others. This material is then applied to organizations to explain the motivations of people and how the potential of the human side of business is best harnessed. This content is a crucial area of knowledge in information systems security management because of the constantly changing security environment and the changing importance of the roles of security officers. Topics such as work motivation, work attitudes, socialization, leadership, decision making, and management of change will all help prepare student for the challenges faced as a security professional or manager.

ISSM 511 Introduction to Information Systems Security

The course covers information systems security issues, policies, practices, and procedures applicable to implementing information systems security on servers. The course also covers the analysis of specific security methods of hardening Microsoft and UNIX operating systems making them highly resistant to penetration. Penetration tests of these hardened servers are undertaken to ensure the effectiveness of the hardening steps taken. The importance and role of physical security measures is also covered.

ISSM 521 TCP/IP Architecture

Full, in-depth coverage of the current TCP/IP protocol (32 bit IPv4). During the course students will implement routed networks with Microsoft or Linux machines acting as routers and populate the network with a variety of operating systems. The course also includes an overview of the new 128 bit version of TCP/IP. Students will install servers and subnets to simulate a network environment that has the capacity to accommodate thousands of users (through the use of built in redundant server roles). Students will also gain experience connecting through an IPv4/IPv6 router to the area of the internet used for testing IPv6 prior to widespread conversion of the internet to IPv6 by approximately 2008. Security issues with both protocols are highlighted in the course as well as methods to overcome these issues.

ISSM 525 Securing an E-Commerce Infrastructure

This course focuses on securing the e-commerce infrastructure, taking into account data architecture and management and advanced network protocols. In the e-commerce environment, both information security needs of organizations and privacy needs of customers and clients are examined.

ISSM 531 Advanced Network Security

This course reviews the network environment and any enterprise resource considerations for planning network connectivity and security. Security components for authentication

access control and security software are highlighted and applied in labs. Protection mechanisms that are designed into operating systems to protect information systems are also discussed and implemented in labs. Students secure web and ftp servers in a lab environment and apply appropriate fixes and patches to ensure the servers are protected to the desired standards. During this course a wide variety of penetration tools will be used to assess weaknesses of network and servers hardened. Students are challenged to use this information to formulate methods of attack which might successfully defeat the protection and counter-measures undertaken. Prerequisites: ISSM 511, 521 and 525.

ISSM 533 Cryptology and Secure Network Communications

This course in cryptography focuses on securing data through authentication, cryptographic algorithms, access control, public key encryption and public key distribution using best practices for secure communications. Students assess and evaluate cryptographic systems and how they can be incorporated into an information security system and the security plan for the enterprise. Students implement secure sites (on web servers) that require secure sockets layer for secure transactions. Emerging trends in encryption are discussed to prepare students for the ongoing changes which will be required to keep ahead of hackers. Prerequisites: ISSM 511, 521 and 525.

ISSM 535 Firewall Fundamentals

Covers both the theory behind firewall technology and the practical implementation in routed IPv4 based TCP/IP based networks. Topics include the planning, formation, management, and operation of security of the firewall itself as well as the other zones it interacts with, such as: the local area network zone used by the organization, the demilitarized zone normally used by the company for servers which must be connected to the internet, and the internet zone which is an untrusted zone. Students also learn how to evaluate the effectiveness of a firewall design. Students implement a firewall and test its effectiveness for load capacity and functionality. Prerequisites: ISSM 511, 521 and 525.

ISSM 536 Forensics

This course is an in-depth analysis of incidence response and forensic sciences that can be applied to computer media in order to determine losses and compromises to the security of information. The course focuses on the gathering of computer data in the case of the misuse of information, the best practices to use in the event of criminal misuse of information, and the implications of privacy legislation in Canada on the use of forensics for determining the possible misuse of information. The techniques used in the course cover a wide variety of operating and file systems; however, the lab work in the course will deal with the most commonly used computer and operating system (Microsoft systems with FAT or NTFS file systems).

ISSM 538 Research Methods I

This course is lecture based and focuses on formulating a research question or research problem, determining research design, assessing data collection methods, determining a sampling framework, determining types of data analyses, and interpreting data. Qualitative and quantitative research methods will be included. Students will gain an understanding of the ethical issues involved in conducting research.

ISSM 539 Research Methods II

This seminar course follows ISSM 538. The students work to determine specific areas of interest and to develop a research plan and research proposal which will later be used (if approved) as the basis to register in either ISSM 570 or ISSM 571. Early in the term, seminars will be the prime method to help the students focus their research interest. Later in the term, one-on-one meetings with the faculty member responsible for the course and/or the program director and the student's advisor will be the main methods used in assisting and directing students in their research goals. Prerequisites: ISSM 538 and consent of the department.

ISSM 541 Financial Management and Analysis

The course focuses on financial management theory and financial statement analysis. Students use rate-of-return, break-even, scenario analysis, and other methods to evaluate projects and organizational performance. Students also learn how to make financial proposals for new equipment needed for an information security enhancement. To a more limited degree, IT security auditing is also discussed along with the importance of IT auditing to the enterprise. Note: Credit may be obtained for only one of ISSM 441 or 541.

ISSM 543 Systems Development and Project Management

An in-depth study of the concepts and techniques for designing, developing and/or revising software using a planned approach. Both the software development life-cycle model and project management approach is presented. Students apply project management concepts in this course to group and individual projects. Note: Credit may be obtained for only one of ISSM 443 or 543.

ISSM 545 Security Policies, Standards and Management

This course provides students with the standards for creating an enterprise-wide network security policy. Topics include: security management principles; defining security requirements; planning and documenting security policies; asset identification and control; system access control; and Internet security. Students also learn how to formulate, administer, manage and evaluate network security policies and standards based on best standards for information systems security (ISO 17799), best practices for security auditing (COBIT) and the protection of private information required by Canadian laws. Note: Credit may be obtained for only one of ISSM 445 or 545.

ISSM 551 Disaster Recovery and Planning

An in-depth coverage of disaster recovery planning including, techniques to prevent, detect, and recover from loss of information availability. Students are instructed in ways to formulate a disaster and recovery plan, and test and implement the plan in a simulated lab environment. Prerequisites: ISSM 511, 521, and 525.

ISSM 553 Risk Management and Analysis

This course focuses on the principles and techniques applied to security risk analysis and the role of risk management in the business enterprise. Topics covered include how to conduct vulnerability assessments, the use of risk assessment tools and how to establish a cost benefit analysis for specific safeguards to ensure that information is confidential, available and has integrity. Emerging trends in risk management are also explored. Students use standard tools to assess network weaknesses such as UNIX-based NMAP and Nessus. These tools are also used in other security courses in the third semester in the program. Note: Credit may be obtained for only one of ISSM 453 or 553.

ISSM 561 Information Technology Law and Ethics

This course provides an overview of International and Canadian laws, legislation, and legal issues relevant to the information systems security profession. Topics covered include the legal protection of information and systems technology, as well as balancing the legal rights to privacy for users. Legal “due diligence” responsibilities of information security professionals are also discussed.

ISSM 570: Practicum Based Research Project

A research project culminating in the production of a formal report and an oral presentation of the student’s research. Each student will conduct his or her research in a professional work environment with the approval and under the supervision of (a) a work-experience supervisor in the sponsoring institution and (b) Concordia’s Information Systems Security Management director or a designate of the director and the Masters Program Committee. Prerequisites: Successful completion of all core ISSM courses and a minimum grade point average of 3.0.

ISSM 571: Research Project in Subject Area

A research project culminating in the production of a formal report and an oral presentation of the student’s research. Each student will conduct his or her research with the approval and under the direction of the student’s faculty supervisor. Each student will conduct his or her research with the approval and under the supervision of a research supervisor, Concordia’s Information Systems Security Management director or a designate of the director and the Masters Program Committee. Prerequisites: Successful completion of all core ISSM courses and a minimum grade point average of 3.0.