



CURRICULUM OVERVIEW

MASTER OF SCIENCE IN INFORMATION SECURITY MANAGEMENT (MSISM)¹

Specializations

- Information Security Analysis (ISA)
- Information Security Auditing (IAU)
- Information System Certification (ISC)
- Information Security Engineering (ISE)
- Information Security Research (ISR)

Description

This degree program prepares students to be strategic and tactical contributors in the development, implementation and evaluation of enterprise level security programs. Specializations allow students to pursue a program of study which relates to their professional interests and goals.

Information Security Analysis (ISA)

Students develop competencies in implementing an enterprise strategic security plan by integrating effective security policies, standards, procedures and controls.

Information Security Auditing (IAU)

Students develop competencies in assessing network vulnerabilities, analyzing cyber evidence, enforcing data process controls, and establishing information protection programs.

Information System Certification (ISC)

Students develop competencies in supporting a management structure to certify and accredit information systems by developing policies, standards and procedures in accordance with a prescribed set of criteria.

Information Security Engineering (ISE)

Students develop competencies in assessing network vulnerabilities and attack methods as well as in designing and deploying counter-measures and resilient security architectures.

Information Security Research (ISR)

Doctoral students who have completed a minimum of 36 semester credits of a University of Fairfax doctoral degree program, but wish to discontinue studies, may be awarded an MSISM degree in *Information Security Research*. Should circumstances change in the future, the student may reapply to a University of Fairfax doctoral program with advanced standing.

¹ Programs of study and course descriptions are subject to change without notice. Unless otherwise indicated all courses are three semester credits.

Program Objectives

- To gain knowledge in a specialized field of study based upon theory, concepts and skills relevant to Information Security practitioners.
- To apply critical thinking and problem-solving skills in the analysis of issues relevant to Information Security practitioners.
- To utilize secondary research competencies in the analysis of issues relevant to Information Security practitioners.
- To develop the necessary skills and perspectives to address a specialized area of Information Security management.

Learning Outcomes

Upon completion of this degree program, students will be able to:

- Compile, analyze, and assess the applicability of best practices in addressing Information Security issues.
- Evaluate the impact of business constraints and processes on the implementation of Information Security programs.
- Integrate principles and techniques of risk analysis, project planning and change management in the development of Information Security strategies.
- Demonstrate secondary research skills in the investigation and selection of best practice solutions to address Information Security challenges.
- Demonstrate mastery of theory, concepts and skills in addressing specialized aspects of Information Security issues.

Credit Requirements

The MSISM degree program consists of 36 semester credits beyond a baccalaureate degree, including 24 credits of core courses and 12 credits of specialization-specific courses.

Multiple Specializations

MSISM degree students may pursue multiple specializations. In addition to the core courses, each specialization requires completion of 12 credits of specialization-specific courses. However, a particular course applies only to one specialization; therefore, additional elective courses are required to fulfill credit requirements for additional specialization(s).

SEQ #	<i>COURSES, OBJECTIVES AND DELIVERABLES</i>
1	<i>IA7020 Information Security Systems and Organizational Behavior and Awareness</i>
	<p><i>In this course, students utilize a subset of five of the ten domains of the (ISC)² Common Body of Knowledge (CBK) in information security as a framework to critically analyze security awareness issues and to evaluate best practices in implementing security systems within the enterprise. (3 credits)</i></p> <p>DELIVERABLES: Best Practice Analyses</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To compare and contrast the mechanisms and procedures used by management to influence behavior, use, and content of an information system. • To propose best practices which utilize the means and methods of disguising information through cryptography in order to protect confidentiality and integrity. • To evaluate the impact of high level procedures, structures and standards used in defining, designing, and implementing information systems and technology. • To analyze structures, transmission methods, transport formats and security measures that enable confidentiality, integrity and availability in business communications. • To assess best practices used in establishing controls, within business applications, that support the security strategy of the enterprise.
2	<i>IA7030 Legal and Ethical Practices in Information Security</i>
	<p><i>In this course, students utilize a subset of five of the ten domains of the (ISC)² Common Body of Knowledge (CBK) in information security as a framework to critically analyze ethical decision-making and to evaluate the best practices employed in security operations planning and management. (3 credits)</i></p> <p>DELIVERABLES: Best Practice Analyses</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To assess associated security risks of various frameworks, policies, and structures of enterprise information assets. • To evaluate physical, procedural, and environmental risks associated with a business information technology infrastructure. • To recommend procedures and best practices required to preserve business in the face of major disruptions to normal operations. • To propose best practices for the protection and control of information technology resources. • To evaluate ethical investigative measures and techniques used to identify and retain evidence of security incidents within the constraints of general computer crime legislation and regulations.
3	<i>IA7040 Information Security and Organizational Change</i>
	<p><i>In this course, students analyze the principles of change management as they apply to the requirements and regulations of information security. Students evaluate the factors which affect corporate decision-making when implementing security programs and the ability of the manager to translate corporate needs into information security projects. (3 credits)</i></p> <p>DELIVERABLE: Change Management Plan</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To analyze the factors influencing the need for change and the imperatives for managing information security change initiatives in the workplace. • To evaluate the need for a specific Information Security change initiative at the group and organizational level. • To evaluate how the proposed change aligns with corporate leadership goals and culture. • To develop a change strategy and identify potential resistance factors to be managed. • To apply appropriate models to implement a sustainable Information Security change initiative.

4	<p><i>RM8250 Web-Based Research Methods in Information Security</i></p> <p><i>In this course, students acquire information retrieval skills and research competencies to identify and evaluate industry-relevant sources of information for the purposes of analysis and research in information security. Students compare and contrast the utility of publicly-available and subscription-based information sources for the purposes of meeting academic and professional requirements. (3 credits)</i></p> <p>DELIVERABLES: Source Analysis; Comparative Analysis of Sources</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To differentiate and classify secondary research sources based on their salient characteristics. • To critically examine the validity and credibility of industry relevant information sources used in information security. • To evaluate and synthesize information sources relating to a topic relevant to information security. • To critically analyze the applicability and relevance of specific information sources for the purposes of meeting academic and professional requirements.
5	<p><i>RM6000 Effective Writing in Information Security Analysis</i></p> <p><i>In this course, students utilize secondary research to analyze a current best practice or process in one of the ten domains of Information Security. Students write and present a white paper providing a rationale for research to evaluate the effectiveness of that practice or process. (3 credits)</i></p> <p>DELIVERABLE: A research white paper related to one of the ten domains.</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To demonstrate effective written and oral communication skills. • To demonstrate knowledge of the secondary research process. • To develop a rationale for applied research in Information Security using literature review. • To demonstrate knowledge of APA requirements for format, source identification and citations in research writing.
6	<p><i>IA8010 Business and Security Risk Analysis</i></p> <p><i>This course provides students with an overview of risk management principles. Methods to identify, quantify, and qualify internal and external risks to the organization are examined. Students apply these principles and methods to the current business and risk environment. (3 credits)</i></p> <p>DELIVERABLES: Case Study Analyses; Business Risk Assessment Report</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To evaluate the role of business and technical risk analysis within the context of Information Security. • To identify and analyze prevalent threats and vulnerabilities facing businesses today. • To identify and analyze business and technical threats to an organization. • To analyze and evaluate Information Security methods used to address business threats and vulnerabilities. • To identify and evaluate the controls necessary to address business and technical threats.
7	<p><i>PM8100 Information Security Project Management</i></p> <p><i>In this course, students utilize PMI's Project Management Body of Knowledge (PMBOK) as a framework to apply project management concepts in the information security arena. Each student develops a project plan for a security assessment which incorporates the technical and behavioral characteristics of high performance teams. (3 credits)</i></p> <p>DELIVERABLES: Project Charter; Work Breakdown Schedule (WBS); Project Plan</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To evaluate the role of project management in improving the success of information technology and information assurance projects. • To demonstrate and apply knowledge of key project management terms and techniques. • To gain experience in the use of project management methodologies and techniques. • To develop skills in creating project management documentation.

8	<i>IA9200 Strategic Analysis in Information Security</i>
	<p><i>In this integrative course, students assess the information security risk associated with an identified management problem. Students then develop a risk mitigation strategy which integrates principles and techniques of risk analysis, project planning, and change management. (3 credits)</i></p> <p>DELIVERABLE: Strategic Risk Mitigation Plan</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To assess the level of risk in an organization with respect to an identified Information Security management problem. • To formulate a strategy to mitigate the identified Information Security risk while limiting liability exposure. • To evaluate the defined strategy to ensure that it either reduces, mitigates, or transfers risk, or results in an acceptable residual risk. • To develop a project plan for implementing the chosen strategy that addresses resources, schedules, and organizational change management requirements.
9	<i>Specialization Course</i>
10	<i>Specialization Course</i>
11	<i>Specialization Course</i>
12	<i>Specialization Course</i>

SPECIALIZATION: INFORMATION SECURITY ANALYSIS

9	<i>IA8120 Information Assurance Policy Planning and Analysis</i> <i>In this course, students develop information assurance policies and deployment plans as part of the comprehensive strategic plan and operational objectives of the enterprise. (3 credits)</i> DELIVERABLES: Enterprise Security Critique; Security Governance Report COURSE OBJECTIVES: <ul style="list-style-type: none">• To analyze how legislation mandates the need for policy.• To identify policy requirements within a given environment.• To develop a policy statement that meets the identified needs.• To formulate an implementation strategy for the policy.
10	<i>IA8020 Security Policies, Standards and Procedures</i> <i>In this course, students examine the role of security policies, standards and procedures in addressing business and technical risks and develop a security governance report to evaluate compliance across the enterprise. (3 credits)</i> DELIVERABLES: Enterprise Security Critique; Security Governance Report COURSE OBJECTIVES: <ul style="list-style-type: none">• To examine the role of security policies, standards and procedures in supporting information security and assurance across the enterprise.• To examine the management of security policy review and implementation projects.• To demonstrate how to effectively address business and technical risks to the enterprise through appropriate policies, standards and procedures.• To develop a security governance report to evaluate compliance across the enterprise.
11	<i>IA8030 Design, Development and Evaluation of Security Controls</i> <i>In this course, students transform high-level policies and procedures into quantifiable and measurable controls and mechanisms that enforce data and process integrity, availability and confidentiality. (3 credits)</i> DELIVERABLES: General IT Controls Review; Application Controls Review COURSE OBJECTIVES: <ul style="list-style-type: none">• To analyze and evaluate the interrelationship between risk management objectives and the application of effective business and IT controls.• To identify, define and evaluate key business and IT processes, requirements and performance metrics used by management to monitor and control risk.• To identify, analyze and evaluate organizational, administrative, network, and application-specific controls and risk mitigation strategies to meet business and technical objectives.• To demonstrate knowledge of the management of business and IT controls assessment projects.• To transform high-level business and technical objectives into quantifiable and measurable controls and mechanisms which enforce data and process integrity, availability and confidentiality.
12	<i>IA8190 Forensic Evaluation and Incident Response Management</i> <i>In this course, students explore the essentials of electronic discovery and analyze issues related to cyber evidence. Using this evidence, students identify and analyze the nature of security incidents, the source of potential threats and the methods used in incident management and mitigation. Students also analyze the technical and business issues which affect the actions of the enterprise in responding to a security incident. (3 credits)</i> DELIVERABLE: Forensic Evaluations; Incident Response Plan COURSE OBJECTIVES: <ul style="list-style-type: none">• To identify and analyze the nature of computer security incidents and the source of potential threats.• To demonstrate knowledge of a methodology for end-to-end incident management and mitigation.• To analyze and evaluate the technical issues associated with incident management and in the identification of criminal actions using network trace back and computer forensics.• To identify, analyze and evaluate the business and non-technical drivers associated with incident management such as legal issues as well as to demonstrate knowledge of the application of the rules of evidence to electronic security incidents.

SPECIALIZATION: INFORMATION SECURITY AUDITING

9	<p><i>IA8050 Security Risk and Vulnerability Assessment</i></p> <p><i>This course provides students with an understanding of advanced techniques and tools for identifying and categorizing vulnerabilities that allow penetration of networked systems and environments. Students gain first-hand experience in the assessment of networked systems through extended virtual lab sessions. (3 credits)</i></p> <p>DELIVERABLES: Security Vulnerability Assessments</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To evaluate the role of basic networking and operating system functions in defining and qualifying security risks. • To demonstrate knowledge of network and system vulnerability assessment terms and techniques. • To utilize standard and advanced tools, techniques and methodologies that support the delivery of network and system vulnerability assessments. • To gain experience in the use of a repeatable methodology for performing detailed network and system vulnerability assessments. • To utilize a systematic approach to testing for vulnerability false-positives.
10	<p><i>IA8190 Forensic Evaluation and Incident Response Management</i></p> <p><i>In this course, students explore the essentials of electronic discovery and analyze issues related to cyber evidence. Using this evidence, students identify and analyze the nature of security incidents, the source of potential threats and the methods used in incident management and mitigation. Students also analyze the technical and business issues which affect the actions of the enterprise in responding to a security incident. (3 credits)</i></p> <p>DELIVERABLE: Forensic Evaluations; Incident Response Plan</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To identify and analyze the nature of computer security incidents and the source of potential threats. • To demonstrate knowledge of a methodology for end-to-end incident management and mitigation. • To analyze and evaluate the technical issues associated with incident management and in the identification of criminal actions using network trace back and computer forensics. • To identify, analyze and evaluate the business and non-technical drivers associated with incident management such as legal issues as well as to demonstrate knowledge of the application of the rules of evidence to electronic security incidents.
11	<p><i>IA8030 Design, Development and Evaluation of Security Controls</i></p> <p><i>In this course, students transform high-level policies and procedures into quantifiable and measurable controls and mechanisms that enforce data and process integrity, availability and confidentiality. (3 credits)</i></p> <p>DELIVERABLES: General IT Controls Review; Application Controls Review</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To analyze and evaluate the interrelationship between risk management objectives and the application of effective business and IT controls. • To identify, define and evaluate key business and IT processes, requirements and performance metrics used by management to monitor and control risk. • To identify, analyze and evaluate organizational, administrative, network, and application-specific controls and risk mitigation strategies to meet business and technical objectives. • To demonstrate knowledge of the management of business and IT controls assessment projects. • To transform high-level business and technical objectives into quantifiable and measurable controls and mechanisms which enforce data and process integrity, availability and confidentiality.
12	<p><i>IA8110 Certification and Accreditation</i></p> <p><i>In this course, students analyze an enterprise-wide view of information systems and the establishment of appropriate, cost-effective information protection programs. Within this context, students examine a set of standard policies, procedures, activities and a management structure to certify and accredit information systems for the protection of the data as well as the systems. (3 credits)</i></p> <p>DELIVERABLES: C&A Plan; Accreditation Recommendation</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To select a certification and accreditation methodology appropriate to an organization’s compliance requirements. • To demonstrate knowledge of the components necessary to perform a certification assessment. • To develop a certification plan to meet an organization’s compliance requirements.

- To assess residual risk and produce an accreditation recommendation.

SPECIALIZATION: INFORMATION SYSTEM CERTIFICATION

9	<p><i>IA8020 Security Policies, Standards and Procedures</i></p> <p><i>In this course, students examine the role of security policies, standards and procedures in addressing business and technical risks and develop a security governance report to evaluate compliance across the enterprise. (3 credits)</i></p> <p>DELIVERABLES: Enterprise Security Critique; Security Governance Report</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To examine the role of security policies, standards and procedures in supporting information security and assurance across the enterprise. • To examine the management of security policy review and implementation projects. • To demonstrate how to effectively address business and technical risks to the enterprise through appropriate policies, standards and procedures. • To develop a security governance report to evaluate compliance across the enterprise.
10	<p><i>IA8030 Design, Development and Evaluation of Security Controls</i></p> <p><i>In this course, students transform high-level policies and procedures into quantifiable and measurable controls and mechanisms that enforce data and process integrity, availability and confidentiality. (3 credits)</i></p> <p>DELIVERABLES: General IT Controls Review; Application Controls Review</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To analyze and evaluate the interrelationship between risk management objectives and the application of effective business and IT controls. • To identify, define and evaluate key business and IT processes, requirements and performance metrics used by management to monitor and control risk. • To identify, analyze and evaluate organizational, administrative, network, and application-specific controls and risk mitigation strategies to meet business and technical objectives. • To demonstrate knowledge of the management of business and IT controls assessment projects. • To transform high-level business and technical objectives into quantifiable and measurable controls and mechanisms which enforce data and process integrity, availability and confidentiality.
11	<p><i>IA8070 Design and Development of Security Architectures</i></p> <p><i>In this course, students evaluate the principles, attributes and processes used in designing and deploying a comprehensive and resilient layered security architecture that supports the business and technical objectives of the enterprise. (3 credits)</i></p> <p>DELIVERABLE: Business Security Plan</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To identify and analyze the key business processes used within the enterprise and the technical implementations of those processes. • To identify, define and evaluate alternative security measures needed to facilitate the previously identified business processes. • To orchestrate the previously identified security measures into an effective, layered security architecture as part of the strategic information technology plan. • To document the design, deployment and implementation of the security architecture in a cohesive business security plan.
12	<p><i>IA8110 Certification and Accreditation</i></p> <p><i>In this course, students analyze an enterprise-wide view of information systems and the establishment of appropriate, cost-effective information protection programs. Within this context, students examine a set of standard policies, procedures, activities and a management structure to certify and accredit information systems for the protection of the data as well as the systems. (3 credits)</i></p> <p>DELIVERABLES: C&A Plan; Accreditation Recommendation</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To select a certification and accreditation methodology appropriate to an organization's compliance requirements. • To demonstrate knowledge of the components necessary to perform a certification assessment. • To develop a certification plan to meet an organization's compliance requirements. • To assess residual risk and produce an accreditation recommendation.

SPECIALIZATION: INFORMATION SECURITY ENGINEERING

9	<p><i>IA8050 Security Risk and Vulnerability Assessment</i></p> <p><i>This course provides students with an understanding of advanced techniques and tools for identifying and categorizing vulnerabilities that allow penetration of networked systems and environments. Students gain first-hand experience in the assessment of networked systems through extended virtual lab sessions. (3 credits)</i></p> <p>DELIVERABLES: Security Vulnerability Assessments</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To evaluate the role of basic networking and operating system functions in defining and qualifying security risks. • To gain knowledge of network and system vulnerability assessment terms and techniques. • To gain experience in the use of standard and advanced tools, techniques and methodologies that support the delivery of network and system vulnerability assessments. • To gain experience in the use of a repeatable methodology for performing detailed network and system vulnerability assessments. • To utilize a systematic approach to testing for vulnerability false-positives.
10	<p><i>IA8060 Intrusion Detection, Attacks and Countermeasures</i></p> <p><i>In this course, students examine common attack methods, technologies and countermeasures. Students also gain skills needed to recognize various stages and methods of attack on the enterprise. (3 credits)</i></p> <p>DELIVERABLES: Network Analysis Report; Intrusion Detection Report; Malware Analysis Report; Firewall Analysis Report</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To analyze network traffic behavior to identify potential hostile activity. • To analyze intrusion detection software alerts and data to identify valid intrusion incidents. • To analyze malware to identify the effects of the malicious behavior on corporate assets. • To assess firewall rule sets and logs to determine validity and potential change requirements.
11	<p><i>IA8070 Design and Development of Security Architectures</i></p> <p><i>In this course, students evaluate the principles, attributes and processes used in designing and deploying a comprehensive and resilient layered security architecture that supports the business and technical objectives of the enterprise. (3 credits)</i></p> <p>DELIVERABLE: Business Security Plan</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To identify and analyze the key business processes used within the enterprise and the technical implementations of those processes. • To identify, define and evaluate alternative security measures needed to facilitate the previously identified business processes. • To orchestrate the previously identified security measures into an effective, layered security architecture as part of the strategic information technology plan. • To document the design, deployment and implementation of the security architecture in a cohesive business security plan.
12	<p><i>IA8080 Security Solution Implementation</i></p> <p><i>In this course, students compare, contrast and evaluate contemporary practices in the implementation of security solutions. (3 credits)</i></p> <p>DELIVERABLES: Security Solution Implementation Plan</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To identify implementation strategies utilized in addressing Information Security problem solutions. • To assess the requirements for each appropriate implementation strategy. • To compare and contrast the benefits and risks associated with alternative implementation strategies in relation to schedule, resources, budget, culture, and compliance requirements. • To formulate a recommended implementation approach and develop the supporting implementation plan documentation.