

## **CURRICULUM OVERVIEW**

### ***GRADUATE CERTIFICATE PROGRAM***

#### **Description**

Graduate certificates represent a level of achievement of technical competencies and project experience which relate to specialized fields of practice in Information Security. Requirements for earning a graduate certificate cannot be satisfied through transfer credit. Upon acceptance into a University of Fairfax degree program, students who have earned a grade of “B” or better in graduate certificate courses may request that those credits be applied to meet degree requirements.

This program fosters the development of students who:

- Are recognized as qualified practitioners in a specialized field of study relevant to the cybersecurity community
- Demonstrate the knowledge and skills necessary to address issues in a specialized area of study in cybersecurity
- Apply critical thinking and problem-solving skills in the performance of tasks associated with a specialized field of study in cybersecurity

#### **Program Objectives**

Upon completion of a graduate certificate, students will be able to:

- Compile, analyze, and assess the applicability of best practices in addressing information security issues
- Demonstrate mastery of theory, concepts and skills in addressing specialized aspects of information security management

#### **Credit Requirements**

Graduate certificates vary from 6 semester credits to 18 semester credits. However, the majority of offerings are 12 credits.

#### **Multiple Graduate Certificates**

Students may earn multiple graduate certificates concurrently or sequentially. Credits earned toward a graduate certificate may also apply to one or more additional graduate certificate(s).

#### **Graduate Certificate Options**

The University of Fairfax offers a variety of graduate certificates to meet the needs of information security professionals.

## **CYBERSECURITY BEST PRACTICES-CISSP (CBP)**

Students explore the ten domains of Information Security and prepare for the CISSP certification exam which demonstrates mastery of subject knowledge in the discipline.

<b><i>IA7020 Information Security Systems and Organizational Behavior and Awareness</i></b>
<i>In this course, students utilize a subset of five of the ten domains of the (ISC)<sup>2</sup> 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>
<b>DELIVERABLES: Best Practice Analyses</b>
<b>COURSE OBJECTIVES:</b>
<ul style="list-style-type: none"><li>• To analyze structures, transmission methods, transport formats and security measures that enable confidentiality, integrity and availability in business communications.</li><li>• To examine best practices which serve to manage and reduce security risks associated with various frameworks, networks and technology structures of an enterprise.</li><li>• To assess best practices used in establishing controls, within business applications, which support the security strategy of an enterprise.</li><li>• To evaluate the impact of high level procedures, structures and standards used in defining, designing, and implementing information systems and technology.</li><li>• To propose best practices which utilize the means and methods of disguising information through cryptography in order to protect confidentiality and integrity of data.</li></ul>
<b><i>IA7030 Legal and Ethical Practices in Information Security</i></b>
<i>In this course, students utilize a subset of five of the ten domains of the (ISC)<sup>2</sup> 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>
<b>DELIVERABLES: Best Practice Analyses</b>
<b>COURSE OBJECTIVES:</b>
<ul style="list-style-type: none"><li>• To evaluate physical, procedural, and environmental risks associated with a business information technology infrastructure.</li><li>• To recommend procedures and best practices required to preserve business in the face of major disruptions to normal operations.</li><li>• To propose best practices for the protection and control of information technology resources.</li><li>• 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.</li></ul>
<b><i>IC7000 (ISC)<sup>2</sup> Official CISSP Review Seminar</i></b>
<i>This course, taught by (ISC)<sup>2</sup> (an authorized education partner of the University) provides students with CBK domain review materials and instructor guidance in preparation for the (ISC)<sup>2</sup> CISSP certification exam. (0 credits)</i>
<b><i>Credits required for Certificate: 6</i></b>

## **INFORMATION SECURITY PROFESSIONAL PRACTICES (ISPP)**

Students develop competencies in assessing threats and vulnerabilities of information systems, designing security procedures and practices that are executed in the protection of data and information systems, and analyzing the validity and reliability of information to ensure that an information system will operate at a proposed level of trust. Upon completion students are awarded the NSA certifications for *Information Systems Security Professionals (CNSS No. 4011)* and *Senior Systems Managers (CNSS No.4012)*.

<p><b><i>IA7020 Information Security Systems and Organizational Behavior and Awareness</i></b></p> <p><i>In this course, students utilize a subset of five of the ten domains of the (ISC)<sup>2</sup> 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><b>DELIVERABLES: Best Practice Analyses</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze structures, transmission methods, transport formats and security measures that enable confidentiality, integrity and availability in business communications.</li><li>• To examine best practices which serve to manage and reduce security risks associated with various frameworks, networks and technology structures of an enterprise.</li><li>• To assess best practices used in establishing controls, within business applications, which support the security strategy of an enterprise.</li><li>• To evaluate the impact of high level procedures, structures and standards used in defining, designing, and implementing information systems and technology.</li><li>• To propose best practices which utilize the means and methods of disguising information through cryptography in order to protect confidentiality and integrity of data.</li></ul>
<p><b><i>IA7030 Legal and Ethical Practices in Information Security</i></b></p> <p><i>In this course, students utilize a subset of five of the ten domains of the (ISC)<sup>2</sup> 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><b>DELIVERABLES: Best Practice Analyses</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To evaluate physical, procedural, and environmental risks associated with a business information technology infrastructure.</li><li>• To recommend procedures and best practices required to preserve business in the face of major disruptions to normal operations.</li><li>• To propose best practices for the protection and control of information technology resources.</li><li>• 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.</li></ul>
<p><b><i>IA8010 Business and Security Risk Analysis</i></b></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><b>DELIVERABLES: Business Risk Assessment Report</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To evaluate the role of business and technical risk analysis within the context of Information Security.</li><li>• To identify and analyze prevalent threats and vulnerabilities facing businesses today.</li><li>• To identify and analyze business and technical threats to an organization.</li><li>• To analyze and evaluate Information Security methods used to address business threats and vulnerabilities.</li><li>• To identify and evaluate the controls necessary to address business and technical threats.</li></ul>

**ISPP CONTINUED**

<p><b>IA8020 Security Policies, Standards and Procedures</b></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><b>DELIVERABLES: Enterprise Security Critique; Security Governance Report</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To examine the role of security policies, standards and procedures in supporting information security and assurance across the enterprise.</li><li>• To examine the management of security policy review and implementation projects.</li><li>• To demonstrate how to effectively address business and technical risks to the enterprise through appropriate policies, standards and procedures.</li><li>• To develop a security governance report to evaluate compliance across the enterprise.</li></ul>
<p><b>IA8030 Design, Development and Evaluation of Security Controls</b></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><b>DELIVERABLES: General IT Controls Review; Application Controls Review</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze and evaluate the interrelationship between risk management objectives and the application of effective business and IT controls.</li><li>• To identify, define and evaluate key business and IT processes, requirements and performance metrics used by management to monitor and control risk.</li><li>• To identify, analyze and evaluate organizational, administrative, network, and application-specific controls and risk mitigation strategies to meet business and technical objectives.</li><li>• To demonstrate knowledge of the management of business and IT controls assessment projects.</li><li>• To transform high-level business and technical objectives into quantifiable and measurable controls and mechanisms which enforce data and process integrity, availability and confidentiality.</li></ul>
<p><b>IA8190 Forensic Evaluation and Incident Response Management</b></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><b>DELIVERABLE: Forensic Evaluations; Incident Response Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To identify and analyze the nature of computer security incidents and the source of potential threats.</li><li>• To demonstrate knowledge of a methodology for end-to-end incident management and mitigation.</li><li>• To analyze and evaluate the business and non-technical drivers as well as technical issues associated with incident management.</li><li>• To apply the rules of evidence to electronic security incidents in the identification of criminal actions using network trace back and computer forensics.</li></ul>
<p><b>Credits required for Certificate: 18</b></p>

## ***INFORMATION SECURITY ANALYSIS (ISA)***

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

<p><b><i>IA8125 Information Security Policy Planning and Analysis</i></b></p> <p><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></p> <p><b>DELIVERABLES: Policy Analysis; Policy Statement; Policy Implementation Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze how legislation mandates the need for policy.</li><li>• To identify policy requirements within a given environment.</li><li>• To develop a policy statement that meets the identified needs.</li><li>• To formulate an implementation strategy for the policy.</li></ul>
<p><b><i>IA8020 Security Policies, Standards and Procedures</i></b></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><b>DELIVERABLES: Enterprise Security Critique; Security Governance Report</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To examine the role of security policies, standards and procedures in supporting information security and assurance across the enterprise.</li><li>• To examine the management of security policy review and implementation projects.</li><li>• To demonstrate how to effectively address business and technical risks to the enterprise through appropriate policies, standards and procedures.</li><li>• To develop a security governance report to evaluate compliance across the enterprise.</li></ul>
<p><b><i>IA8030 Design, Development and Evaluation of Security Controls</i></b></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><b>DELIVERABLES: General IT Controls Review; Application Controls Review</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze and evaluate the interrelationship between risk management objectives and the application of effective business and IT controls.</li><li>• To identify, define and evaluate key business and IT processes, requirements and performance metrics used by management to monitor and control risk.</li><li>• To identify, analyze and evaluate organizational, administrative, network, and application-specific controls and risk mitigation strategies to meet business and technical objectives.</li><li>• To demonstrate knowledge of the management of business and IT controls assessment projects.</li><li>• To transform high-level business and technical objectives into quantifiable and measurable controls and mechanisms which enforce data and process integrity, availability and confidentiality.</li></ul>
<p><b><i>IA8190 Forensic Evaluation and Incident Response Management</i></b></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><b>DELIVERABLE: Forensic Evaluations; Incident Response Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To identify and analyze the nature of computer security incidents and the source of potential threats.</li><li>• To demonstrate knowledge of a methodology for end-to-end incident management and mitigation.</li><li>• To analyze and evaluate the business and non-technical drivers as well as technical issues associated with incident management.</li><li>• To apply the rules of evidence to electronic security incidents in the identification of criminal actions using network trace back and computer forensics.</li></ul>
<p><b><i>Credits required for Certificate: 12</i></b></p>

## **INFORMATION SECURITY AUDITING (IAU)**

Students develop competencies in forensically analyzing cyber evidence, enforcing data process controls, certifying information protection programs, and managing risk and compliance.

<p><b><i>IA8030 Design, Development and Evaluation of Security Controls</i></b></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><b>DELIVERABLES: General IT Controls Review; Application Controls Review</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze and evaluate the interrelationship between risk management objectives and the application of effective business and IT controls.</li><li>• To identify, define and evaluate key business and IT processes, requirements and performance metrics used by management to monitor and control risk.</li><li>• To identify, analyze and evaluate organizational, administrative, network, and application-specific controls and risk mitigation strategies to meet business and technical objectives.</li><li>• To demonstrate knowledge of the management of business and IT controls assessment projects.</li><li>• To transform high-level business and technical objectives into quantifiable and measurable controls and mechanisms which enforce data and process integrity, availability and confidentiality.</li></ul>
<p><b><i>IA8110 Certification and Accreditation</i></b></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><b>DELIVERABLES: C&amp;A Plan; Accreditation Recommendation</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To select a certification and accreditation methodology appropriate to an organization's compliance requirements.</li><li>• To demonstrate knowledge of the components necessary to perform a certification assessment.</li><li>• To develop a certification plan to meet an organization's compliance requirements.</li><li>• To assess residual risk and produce an accreditation recommendation.</li></ul>
<p><b><i>IA8190 Forensic Evaluation and Incident Response Management</i></b></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><b>DELIVERABLE: Forensic Evaluations; Incident Response Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To identify and analyze the nature of computer security incidents and the source of potential threats.</li><li>• To demonstrate knowledge of a methodology for end-to-end incident management and mitigation.</li><li>• To analyze and evaluate the business and non-technical drivers as well as technical issues associated with incident management.</li><li>• To apply the rules of evidence to electronic security incidents in the identification of criminal actions using network trace back and computer forensics.</li></ul>
<p><b><i>IA8210 Risk Management and Compliance</i></b></p> <p><i>In this course, students evaluate the procedures and results of risk analysis, as well as compliance processes which address the regulatory requirements that drive the need for risk analysis within the enterprise. Security-related regulations such as SOX, GLBA, FISMA and HIPAA are examined (3 credits)</i></p> <p><b>DELIVERABLE: Security Audit Report; Risk Mitigation Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze security-related regulations and policies and formulate appropriate compliance requirements.</li><li>• To assess the security posture of an organization and perform a compliance audit.</li><li>• To analyze the risks associated with deficiencies identified in the compliance audit.</li><li>• To develop a mitigation plan to achieve compliance.</li></ul>
<p><b><i>Credits required for Certificate: 12</i></b></p>

## **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.

<p><b><i>IA8030 Design, Development and Evaluation of Security Controls</i></b></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><b>DELIVERABLES: General IT Controls Review; Application Controls Review</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze and evaluate the interrelationship between risk management objectives and the application of effective business and IT controls.</li><li>• To identify, define and evaluate key business and IT processes, requirements and performance metrics used by management to monitor and control risk.</li><li>• To identify, analyze and evaluate organizational, administrative, network, and application-specific controls and risk mitigation strategies to meet business and technical objectives.</li><li>• To demonstrate knowledge of the management of business and IT controls assessment projects.</li><li>• To transform high-level business and technical objectives into quantifiable and measurable controls and mechanisms which enforce data and process integrity, availability and confidentiality.</li></ul>
<p><b><i>IA8110 Certification and Accreditation</i></b></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><b>DELIVERABLES: C&amp;A Plan; Accreditation Recommendation</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To select a certification and accreditation methodology appropriate to an organization's compliance requirements.</li><li>• To demonstrate knowledge of the components necessary to perform a certification assessment.</li><li>• To develop a certification plan to meet an organization's compliance requirements.</li><li>• To assess residual risk and produce an accreditation recommendation.</li></ul>
<p><b><i>IA8140 Business Continuity Planning and Recovery</i></b></p> <p><i>In this course, students explore tools and strategies for Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) activities. Topics include business impact assessment methods, recovery strategy approaches and solutions and continuity planning. (3 credits)</i></p> <p><b>DELIVERABLE: Business Continuity Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To examine methods used in the identification of vulnerabilities and approaches taken to prevent and mitigate risks for an organization.</li><li>• To demonstrate how to effectively address business and technical risks to the enterprise through appropriated business continuity planning and disaster recovery planning activities.</li><li>• To gain experience in the use of standard and advanced tools, techniques and methodologies that support disaster recovery activities.</li></ul>
<p><b><i>IA8190 Forensic Evaluation and Incident Response Management</i></b></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><b>DELIVERABLE: Forensic Evaluations; Incident Response Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To identify and analyze the nature of computer security incidents and the source of potential threats.</li><li>• To demonstrate knowledge of a methodology for end-to-end incident management and mitigation.</li><li>• To analyze and evaluate the business and non-technical drivers as well as technical issues associated with incident management.</li><li>• To apply the rules of evidence to electronic security incidents in the identification of criminal actions using network trace back and computer forensics.</li></ul>
<p><b><i>Credits required for Certificate: 12</i></b></p>

## **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.

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

## **INFORMATION SECURITY FOR THE ENTERPRISE (ISEN)**

Students explore the ten domains of Information Security and examine effective approaches to implementing security awareness programs within an enterprise.

<p><b>IA7020 Information Security Systems and Organizational Behavior and Awareness</b></p> <p><i>In this course, students utilize a subset of five of the ten domains of the (ISC)<sup>2</sup> 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><b>DELIVERABLES: Best Practice Analyses</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze structures, transmission methods, transport formats and security measures that enable confidentiality, integrity and availability in business communications.</li><li>• To examine best practices which serve to manage and reduce security risks associated with various frameworks, networks and technology structures of an enterprise.</li><li>• To assess best practices used in establishing controls, within business applications, which support the security strategy of an enterprise.</li><li>• To evaluate the impact of high level procedures, structures and standards used in defining, designing, and implementing information systems and technology.</li><li>• To propose best practices which utilize the means and methods of disguising information through cryptography in order to protect confidentiality and integrity of data.</li></ul>
<p><b>IA7030 Legal and Ethical Practices in Information Security</b></p> <p><i>In this course, students utilize a subset of five of the ten domains of the (ISC)<sup>2</sup> 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><b>DELIVERABLES: Best Practice Analyses</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To evaluate physical, procedural, and environmental risks associated with a business information technology infrastructure.</li><li>• To recommend procedures and best practices required to preserve business in the face of major disruptions to normal operations.</li><li>• To propose best practices for the protection and control of information technology resources.</li><li>• 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.</li></ul>
<p><b>PM8100 Information Security Project Management</b></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><b>DELIVERABLES: Project Charter; Project Scope Document; Project Management Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To evaluate the role of project management in improving the success of information technology and information assurance projects.</li><li>• To demonstrate and apply knowledge of key project management terms and techniques.</li><li>• To gain experience in the use of project management methodologies and techniques.</li><li>• To develop skills in creating project management documentation.</li></ul>
<p><b>IA7040 Information Security and Organizational Change</b></p> <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><b>DELIVERABLE: Change Management Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze the factors influencing the need for change and the imperatives for managing information security change initiatives in the workplace.</li><li>• To evaluate the need for a specific Information Security change initiative at the group and organizational level.</li><li>• To evaluate how the proposed change aligns with corporate leadership goals and culture.</li><li>• To develop a change strategy and identify potential resistance factors to be managed.</li><li>• To apply appropriate models to implement a sustainable Information Security change initiative.</li></ul>
<p><b>Credits required for Certificate: 12</b></p>

## **CERTIFIED CYBERSECURITY RESEARCHER (CCR)**

Students examine the emerging trends that pertain to security programs, technology, and regulation while developing skills necessary to implement Information Security research projects.

<p><b><i>RM8250 Web-Based Research Methods in Information Security</i></b></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><b>DELIVERABLES: Comparative Analysis of Sources; Resource Evaluations</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To differentiate and classify secondary research sources based on their salient characteristics.</li><li>• To critically examine the validity and credibility of industry relevant information sources used in information security.</li><li>• To evaluate and synthesize information sources relating to a topic relevant to information security.</li><li>• To critically analyze the applicability and relevance of specific information sources for the purposes of meeting academic and professional requirements.</li></ul>
<p><b><i>RM6000 Effective Writing in Information Security Analysis</i></b></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 position paper providing a rationale for research to evaluate the effectiveness of that practice or process. (3 credits)</i></p> <p><b>DELIVERABLE: Annotated Bibliography; Best Practice Research Recommendation</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To demonstrate effective written and oral communication skills.</li><li>• To demonstrate knowledge of the secondary research process.</li><li>• To develop a rationale for applied research in Information Security using literature review.</li><li>• To demonstrate knowledge of APA requirements for format, source identification and citations in research writing.</li></ul>
<p><b><i>RM8500 Research Foundations for the Information Security Practitioner</i></b></p> <p><i>In this course, doctoral students are introduced to the purpose and nature of primary research in Information Security. Students explore the foundations and concepts of applied field research. The Qualifying Exam is administered at the end of this course. (3 credits)</i></p> <p><b>DELIVERABLE: Research Practice Sets</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To understand the research paradigm and how it applies to the field research process</li><li>• To assess what constitutes a non-trivial and feasible research problem</li><li>• To formulate appropriate research questions for field research studies</li><li>• To distinguish the characteristics of dependent and independent variables</li><li>• To construct testable hypotheses appropriate for field research</li></ul>

***And at least two of the following:***

<p><b><i>CEX8220 Security Program Strategies and Implementation (Level I)</i></b></p> <p><i>In this course, students explore the components of a security program for an enterprise and develop a strategy for its implementation. Students must complete a written exam paper which demonstrates mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. (3 credits)</i></p> <p><b>DELIVERABLES: Security Program Review; Research Paper</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To evaluate the role the security program plays in defining the security posture of the enterprise.</li><li>• To demonstrate knowledge of the approaches taken in implementation of a security program.</li><li>• To develop an implementation plan to meet compliance requirements of an identified security program.</li><li>• To develop a plan for implementing the chosen strategy that addresses resources, schedules, and organizational change management requirements.</li></ul>
---

**CCR CONTINUED**

<p><b><i>CEX8230 Legal and Ethical Management Issues in Information Security (Level I)</i></b></p> <p><i>In this course, students explore issues with respect to the legal and regulatory environment of security and the challenges faced in developing and managing policy related to enterprise security. Students must complete a written exam paper which demonstrates mastery of literature-based research skills and APA format and citation requirements. (3 credits)</i></p> <p><b>DELIVERABLES: Regulatory Analysis; Research Paper</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To analyze how legislation influences specific corporate or institutional environments.</li><li>• To identify legal and ethical issues that arise within a given legal or regulatory environment.</li><li>• To investigate best practices that address specific issues within a given legal or regulatory environment.</li></ul>
<p><b><i>CEX8240 Strategic and Technological Trends in Information Security (Level I)</i></b></p> <p><i>In this course, students assess and evaluate technical trends and emerging technologies in information assurance and examine their impact on the implementation of security programs. Students must complete a written exam paper which demonstrates mastery of literature-based research skills and APA format and citation requirements. (3 credits)</i></p> <p><b>DELIVERABLES: Technology Review; Research Paper</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To gain knowledge of new and emerging technologies available to address initiatives identified in the security program of an enterprise.</li><li>• To gain exposure to technologies currently used in the implementation of the security program.</li><li>• To assess trends in technology and their impact on the implementation of the security program.</li></ul>
<p><b><i>CEX9200 Research Topics in Information Security (Level II)</i></b></p> <p><i>In this course, doctoral students enrolled in the DSc program must complete a written research exam paper which demonstrates mastery of a selected CBK domain, literature-based research skills and APA format and citation requirements. (3 credits)</i></p> <p><b>DELIVERABLES: Research Paper</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To demonstrate mastery of literature-based research skills and APA documentation and citation formats.</li><li>• To demonstrate mastery in selected domains within the Common Body of Knowledge (CBK) in Information Security.</li></ul>
<p><b><i>Credits required for Certificate: 15</i></b></p>

## ***INFORMATION SECURITY RESEARCH PRACTICES (ISRP)***

Students explore concepts and foundations of applied research, identify a feasible research site, and utilize industry-relevant problems to propose an original field research study.

<p><b><i>RM8250 Web-Based Research Methods in Information Security</i></b></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><b>DELIVERABLES: Comparative Analysis of Sources; Resource Evaluations</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To differentiate and classify secondary research sources based on their salient characteristics.</li><li>• To critically examine the validity and credibility of industry relevant information sources used in information security.</li><li>• To evaluate and synthesize information sources relating to a topic relevant to information security.</li><li>• To critically analyze the applicability and relevance of specific information sources for the purposes of meeting academic and professional requirements.</li></ul>
<p><b><i>RM6000 Effective Writing in Information Security Analysis</i></b></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 position paper providing a rationale for research to evaluate the effectiveness of that practice or process. (3 credits)</i></p> <p><b>DELIVERABLE: Annotated Bibliography; Best Practice Research Recommendation</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To demonstrate effective written and oral communication skills.</li><li>• To demonstrate knowledge of the secondary research process.</li><li>• To develop a rationale for applied research in Information Security using literature review.</li><li>• To demonstrate knowledge of APA requirements for format, source identification and citations in research writing.</li></ul>
<p><b><i>RM8500 Research Foundations for the Information Security Practitioner</i></b></p> <p><i>In this course, doctoral students are introduced to the purpose and nature of primary research in Information Security. Students explore the foundations and concepts of applied field research. The Qualifying Exam is administered at the end of this course. (3 credits)</i></p> <p><b>DELIVERABLE: Research Practice Sets</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To understand the research paradigm and how it applies to the field research process</li><li>• To assess what constitutes a non-trivial and feasible research problem</li><li>• To formulate appropriate research questions for field research studies</li><li>• To distinguish the characteristics of dependent and independent variables</li><li>• To construct testable hypotheses appropriate for field research</li></ul>
<p><b><i>RM9100 Qualitative and Quantitative Analysis</i></b></p> <p><i>In this course, students compare, contrast, and evaluate qualitative and quantitative methods of data analysis for solving information assurance problems and conducting information security-related field research. (3 credits)</i></p> <p><b>DELIVERABLES: Questionnaire Quality Assessment; Data Collection and Analysis Report</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To evaluate the applicability of qualitative versus quantitative analysis methods.</li><li>• To determine when parametric versus non-parametric statistics should be used.</li><li>• To utilize qualitative and quantitative analytical methods in evaluating Information Security case studies.</li></ul>
<p><b><i>RM9150 Feasible Problem-Driven Research in Information Security</i></b></p> <p><i>In this course, students identify a research site and utilize problems occurring there in order to identify feasible topic areas for their field research study. Students apply the concept of problem-driven research as the basis for selecting a feasible and non-trivial research topic or problem assessment. (3 credits)</i></p> <p><b>DELIVERABLES: Research Site Access Plan</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To understand what constitutes an acceptable research site.</li><li>• To select an accessible site at which to conduct research.</li><li>• To determine the nature and degree of access to the potential subjects to be studied.</li><li>• To understand the constraints and limitations of the identified research site.</li><li>• To understand the role of a mentor /advocate at the research site.</li></ul>

**ISRP CONTINUED**

**And at least one of the following:**

<b>RM9200 Designing Solutions to Information Security Problems</b>
<i>In this course, doctoral students enrolled in the DIA program continue to evaluate the feasibility of their proposed research site and the potential solutions to be studied. Students present their proposed project at the Dissertation Bootcamp at the end of this course. (3 credits)</i>
<b>DELIVERABLE: Research Project Feasibility Analysis</b>
<b>COURSE OBJECTIVES:</b>
<ul style="list-style-type: none"><li>• To identify potential problems affecting the research population.</li><li>• To recognize potential solutions which address the problems identified.</li><li>• To formulate an acceptable research question applicable to a feasibility assessment of a proposed solution.</li><li>• To articulate a problem statement that will be addressed by the proposed study.</li><li>• To select a researchable topic area (site, problem, Information Security domain).</li></ul>
<b>RM9250 Building a Knowledge-Base in the Information Security Discipline</b>
<i>In this course, doctoral students enrolled in the DSc program continue to evaluate the feasibility of their proposed research site, the research topic identified, and the potential dependent variables to be studied. Students present their proposed project at the Dissertation Bootcamp at the end of this course. (3 credits)</i>
<b>DELIVERABLE: Research Project Feasibility Analysis</b>
<b>COURSE OBJECTIVES:</b>
<ul style="list-style-type: none"><li>• To identify potential problems affecting the research population.</li><li>• To recognize potential dependent variables that can be studied.</li><li>• To formulate an acceptable research question applicable to the problem being studied.</li><li>• To articulate a problem statement that will be addressed by the proposed study.</li><li>• To select a researchable topic area (site, problem, Information Security domain).</li></ul>
<b>Credits required for Certificate: 18</b>

## **KNOWLEDGE-BASED RESEARCH FOR INFORMATION SECURITY PRACTITIONERS (KRIS)**

Students learn how to articulate a research problem, conduct a research literature review, and synthesize relevant research in the development of an original Information Security research project derived from theory and practice. (*DSc students only*)

<b><i>RES8510 Research Topic Rationale</i></b>
<p><i>In this course, students articulate the business problem and problem statement which will be addressed by their research project. In addition, they conduct a preliminary literature review to develop the rationale for their research and the research questions that will guide their study. (3 credits)</i></p> <p><b>DELIVERABLE: Research Rationale (Chapter 1).</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To identify the problem to be addressed by the field research study.</li><li>• To conduct a preliminary review of literature to substantiate that the problem has relevance beyond the research site.</li><li>• To establish the rationale and research objectives for conducting the proposed research.</li><li>• To formulate an appropriate research question to guide the proposed study.</li></ul>
<b><i>RES8520 Review and Synthesis of Prior Research</i></b>
<p><i>In this course, students expand the literature review and synthesize relevant empirical research in order to provide justification for the proposed research. In so doing, students narrow the focus of the proposed topic, formulate the final research question, identify the opportunity to contribute to knowledge in the Information Security arena, and describe the theoretical foundation for their research study. (3 credits)</i></p> <p><b>DELIVERABLE: Literature Review and Synthesis (Chapter 2)</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To conduct a review of empirical research with respect to the proposed research topic.</li><li>• To identify all variables (dependent, independent, parameters) relevant to the proposed research.</li><li>• To formulate hypotheses relevant to the proposed research.</li><li>• To synthesize the findings of the reviewed literature to serve as the theoretical foundation for the proposed research.</li><li>• To construct a conceptual model which describes the relationships among and between the study variables.</li><li>• To articulate the final research question and the justification for the proposed research.</li></ul>
<b><i>RES8530 Proposed Research Methodology</i></b>
<p><i>In this course, students operationally define the study variables, identify the measures of these variables and justify the approach to be taken in the study (qualitative vs. quantitative, exploratory vs. hypothesis-testing). Students document their proposal with the completion of the Proposed Research Plan (PRP). (3 credits)</i></p> <p><b>DELIVERABLE: Proposed Research Plan (PRP) (Chapters 1, 2, and 3.1 through 3.4)</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To define operational measures of study variables.</li><li>• To describe the context of the study including setting, population and sample.</li><li>• To identify and justify the design approach of the study (qualitative vs. quantitative; exploratory vs. hypothesis-testing)</li></ul>
<b><i>RES8550 Research Design: Data Collection Plan</i></b>
<p><i>In this course, students develop the data collection plan based upon the selected research approach and design type. This plan specifies the methods to be utilized for measuring the variables as well as the data collection procedures to be followed. (3 credits)</i></p> <p><b>DELIVERABLE: Research Design, Data Collection Plan (Chapter 3.5 through 3.6)</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To specify the design of the study using an established model.</li><li>• To identify or produce reliable, valid instrument(s) for use in data collection.</li><li>• To specify the detailed data collection procedures to be used.</li><li>• To describe the pilot test of the selected instrument(s).</li></ul>

**KRIS CONTINUED**

<p><b><i>RES8560 Research Design: Results and Findings</i></b></p> <p><i>In this course, students develop the data analysis plan based upon the selected research approach and design type. This plan specifies the data analysis methods and procedures to be utilized in the research. (3 credits)</i></p> <p><b>DELIVERABLE: Data Analysis Plan (Chapter 4.1)</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To specify the methods to be used in analysis of the data.</li><li>• To explain the rationale of the selection of the identified methods of analysis.</li><li>• To describe the treatment for missing data.</li></ul>
<p><b><i>RES8570 Research Design Specification</i></b></p> <p><i>In this course, students finalize the operational requirements of the proposed research study by producing the Research Design Specification (RDS). (3 credits)</i></p> <p><b>DELIVERABLE: Research Design Specification (RDS) (Chapters 1, 2, 3, and 4.1)</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To integrate all previous work into the final specifications of the research design.</li><li>• To obtain IRB approval of the Data Collection Plan and instruments.</li></ul>
<p><b><i>Credits required for Certificate: 18</i></b></p>

## ***SOLUTION-BASED RESEARCH FOR INFORMATION SECURITY PRACTITIONERS (SRIS)***

Students learn how to articulate a research problem, conduct a research literature review, and synthesize relevant research in the development of a solution-based Information Security research project. *(DIA students only)*

<b><i>RES8110 Research Needs and Requirements Analysis</i></b>
<p><i>In this course, students articulate the business problem and problem statement, refine their research question, and develop the rationale for the research project by clearly identifying and specifying the needs and requirements which justify a proposed improvement in professional practice. (3 credits)</i></p> <p><b>DELIVERABLE: Research Rationale (Chapter 1).</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To articulate the specific problem to be addressed by the field research study.</li><li>• To perform a preliminary literature search to identify an evidence-based solution or practice to address the problem.</li><li>• To establish the rationale and research objectives for conducting the proposed research.</li><li>• To formulate an appropriate research question to guide the proposed study.</li></ul>
<b><i>RES8120 Identification of Evidence-Based Solutions</i></b>
<p><i>In this course, students conduct a literature review in Information Security and other relevant bodies of research to identify a proposed solution to the business problem. Using this literature review, they present support for the selection of the proposed solution and identify criteria to be used in assessing its feasibility. (3 credits)</i></p> <p><b>DELIVERABLE: Research Review and Synthesis (Chapter 2)</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To conduct a review of empirical research with respect to the identified problem and previous resolution attempts.</li><li>• To analyze the findings of the reviewed literature to develop evidence-based recommendations for solutions to the identified problem.</li><li>• To synthesize the findings of the reviewed literature to identify criteria that will serve to determine feasibility of the proposed solution.</li><li>• To evaluate solution options and feasibility criteria to select a proposed solution to be studied.</li></ul>
<b><i>RES8130 Operational Design and Specification</i></b>
<p><i>In this course, students finalize the operational requirements of the proposed research study and specify their proposed improvement in professional practice. Students document the methodology to be utilized in the proposed project in the Feasibility Study Specification (FSS) which is the final course deliverable. (3 credits)</i></p> <p><b>DELIVERABLE: Feasibility Study Specification (Chapters 1, 2, 3.1-3.4, and 4.1)</b></p> <p><b>COURSE OBJECTIVES:</b></p> <ul style="list-style-type: none"><li>• To identify the context of the study including setting, population and sample.</li><li>• To identify or produce reliable, valid data collection methods and instrumentation.</li><li>• To specify the detailed data collection procedures to be used.</li><li>• To specify the methods of analysis that will be used during the study.</li></ul>
<b><i>Credits required for Certificate: 9</i></b>