

CURRICULUM OVERVIEW

DOCTOR OF SCIENCE IN INFORMATION ASSURANCE¹

Description:

This degree program helps students to advance their Information Assurance careers in government, industry or academia. Students develop field research competencies that enable them to undertake applied research that results in a theoretical contribution to the field of Information Assurance.

Program Objectives

- To gain expertise in a specialized field of study based upon theory, concepts and skills relevant to Information Assurance practitioners.
- To apply critical thinking and problem-solving skills in the exploration of a specialized field of study relevant to Information Assurance research.
- To utilize secondary research competencies in developing the rationale and support for conducting primary research relevant to Information Assurance practitioners.
- To demonstrate mastery of literature-based research skills, documentation and citation requirements through the completion of Level I Comprehensive Exams.
- To demonstrate mastery of selected domains within the Common Body of Knowledge (CBK) in Information Security through the completion of Level II Comprehensive Exams.
- To develop primary field research competencies that can result in an “industry driven” contribution to knowledge in a specialized field of study relevant to Information Assurance practitioners.
- To contribute new Information Assurance knowledge by conducting an *a priori* hypothesis test which extends prior empirically developed theoretical research.

Learning Outcomes

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

- Analyze, assess and critique the applicability of best practices in addressing Information Assurance issues.
- Integrate the core concepts of risk analysis, project planning, and change management in the development of Information Assurance strategies.
- Establish the rationale and objectives for conducting primary research in a specialized area of Information Assurance.
- Demonstrate knowledge and synthesis of the current body of literature with respect to a specialized area of Information Assurance.
- Apply appropriate hypothesis testing methodologies and analysis techniques in conducting theory driven primary field research in a specialized area of Information Assurance designed to test and advance theory and theoretical concepts.
- Contribute to the body of knowledge through the documentation of hypothesis testing research methods and findings resulting from conducting primary field research in a specialized area of Information Assurance.

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

Qualifying Exam

Doctoral students enrolled in the DSc program must pass the Qualifying Exam. This exam, which is the required deliverable for the RM6000 course, consists of a five-eight page position paper which describes the rationale and support for a proposed research project to evaluate the effectiveness of a best practice or process employed in one of the 10 Information Security domains known as the Common Body of Knowledge (CBK).

Comprehensive Exams (Level I and II)

Doctoral students enrolled in the DSc program must pass Level I and Level II Comprehensive Exams.

The Level I Comprehensive Exams consist of three 25-30 page research papers on a specified topic in Information Security, which are the required deliverables for IA8220, IA8230 and IA8240; the exams must demonstrate mastery of content and literature-based research skills, while utilizing APA format and citation requirements.

The Level II Comprehensive Exams consist of two 25-30 page papers addressing research questions relating to two of the 10 Information Security domains known as the Common Body of Knowledge (CBK). The exams must demonstrate mastery of the subject matter content as well as literature-based research skills, while utilizing APA format and citation requirements.

If necessary, students may repeat any or all of the Level I or Level II Comprehensive Exams.

Credit Requirements

The *Doctor of Science in Information Assurance* consists of a minimum of 70 semester credits beyond a Master's degree, including 66 credits of pre-dissertation courses (21 credits of Information Security content taken from core and specialization courses, 15 credits of research methods courses, 12 credits of comprehensive exam courses, 18 credits of research-preparation courses) and 4 credits of dissertation development courses.

Specialization Option

DSc students may elect to include a specialization in their program of study. The specialization requires completion of four additional specialization-specific courses. This increases the minimum number of credits required for the degree to 82. Students may choose a specialization from among those that are offered as part of the MSISM degree program, with the exception of the *Information Security Research* (ISR) specialization.

SEQ #	COURSES, OBJECTIVES AND DELIVERABLES
1	<i>IA7020 Information Security Systems and Organizational 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>IA8010 Business and Security Risk Analysis</i>
	<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.

4	<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.
5	<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.
6	<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.

7	<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.
8	<p><i>RM6000 Effective Writing in Information Security Analysis (Qualifying Exam)</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.
9	<p><i>IA9200 Strategic Analysis in Information Security</i></p> <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.
10	<p><i>IA8220 Security Program Strategies and Implementation (Comprehensive Exam -Level I)</i></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, 6th edition (APA) format and citation requirements. (3 credits)</i></p> <p>DELIVERABLES: Security Program Review; Security Implementation Plan; Research Paper</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To evaluate the role the security program plays in defining the security posture of the enterprise. • To demonstrate knowledge of the approaches taken in implementation of a security program. • To develop an implementation plan to meet compliance requirements of an identified security program. • To develop a plan for implementing the chosen strategy that addresses resources, schedules, and organizational change management requirements.

111	<i>IA8230 Legal and Ethical Management Issues in Information Security (Comprehensive Exam -Level I)</i>
	<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>DELIVERABLES: Regulatory Analysis; Research Paper</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To analyze how legislation influences specific corporate or institutional environments. • To identify legal and ethical issues that arise within a given legal or regulatory environment. • To investigate best practices that address specific issues within a given legal or regulatory environment.
12	<i>IA8240 Strategic and Technological Trends in Information Security (Comprehensive Exam -Level I)</i>
	<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>DELIVERABLES: Technology Review; Research Paper</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To gain knowledge of new and emerging technologies available to address initiatives identified in the security program of an enterprise. • To gain exposure to technologies currently used in the implementation of the security program. • To assess trends in technology and their impact on the implementation of the security program.
13	<i>CEX9100 Comprehensive Exams – Level II</i>
	<p><i>In this course, doctoral students enrolled in the DSc program must complete two written research exam papers which demonstrate mastery of the selected CBK domains, literature-based research skills and APA format and citation requirements. (3 credits)</i></p> <p>DELIVERABLES: Exam Papers</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To demonstrate mastery of literature-based research skills and APA documentation and citation formats. • To demonstrate mastery in selected domains within the Common Body of Knowledge (CBK) in Information Security.
PHASE I	IDENTIFYING A DISSERTATION TOPIC
Step 1	Understanding the Dissertation Research Process
	<i>RM8250 Web-Based Research Methods in Information Security</i>
	<ul style="list-style-type: none"> • Completed in sequence #7
	<i>RM6000 Effective Writing in Information Security Analysis</i>
	<ul style="list-style-type: none"> • Completed in sequence #8
	<i>Orientation to the University of Fairfax Dissertation Process</i>
	<p><i>During this orientation, an advisor facilitates a review of the Dissertation Handbook with doctoral students.</i></p> <p>ORIENTATION OBJECTIVE:</p> <ul style="list-style-type: none"> • To help students understand and prepare for the requirements of the dissertation process. • To familiarize students with the Dissertation Handbook as a resource to utilize throughout the DPP.

Step 2	Understanding Research Principles and Techniques
	<i>RM9100 Qualitative and Quantitative Analysis</i>
	<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>DELIVERABLES: Questionnaire Quality Assessment; Data Collection and Analysis Plan</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To evaluate the applicability of qualitative versus quantitative analysis methods. • To determine when parametric versus non-parametric statistics should be used. • To utilize qualitative and quantitative analytical methods in evaluating Information Security case studies.
	<i>RM9150 Feasible Problem-Driven Research in Information Security</i>
	<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. (3 credits)</i></p> <p>DELIVERABLES: Draft Research Project Feasibility Analysis (RPFA)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To understand what constitutes an acceptable research site. • To identify an accessible site at which to conduct research. • To determine the nature and degree of access to the potential subjects to be studied. • To understand the constraints and limitations of the identified research site. • To understand the role of a mentor/advocate at the research site. • To select a researchable topic area (site, problem, Information Security domain). • To identify the dependent variable that can be studied at the research site.
	<i>RM9300 Applying the Empirical Research Paradigm to Information Security</i>
	<p><i>In this course, doctoral students utilize empirical research paradigm as a model and identify implications for its application to their proposed research. Students continue to evaluate the feasibility of their proposed research site and the research topic identified. Finally students identify the independent and dependent variables to be studied. (3 credits)</i></p> <p>DELIVERABLE: Research Project Feasibility Analysis (RPFA)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To understand the research paradigm in order to utilize it in the field research process. • To understand the factors determining the feasibility of a field research project. • To analyze the role of site selection in defining a researchable (non-trivial, feasible) field research project.
Step 3	Obtaining Approval for a Feasible Problem-Driven Research Topic
	<i>Dissertation Bootcamp - Presentation of Dissertation Topic</i>
	<p><i>Students present their topic selections and feasibility analyses to the Dean of Doctoral Research and invited faculty. This presentation includes the context of the study, the feasibility of the research site, the topic to be researched, and the dependent variable. If the topic is approved, a Dissertation Committee Chair is appointed prior to the start of the next course.</i></p> <p>BOOTCAMP OBJECTIVE:</p> <ul style="list-style-type: none"> • To obtain approval of the research topic. • To be assigned a Dissertation Committee Chair.

PHASE II	ACHIEVING CANDIDACY
Step 4	Developing the Proposed Research Plan (PRP)
	<i>RES9110 Research Topic Rationale</i>
	<p><i>In this course, students articulate the business problem and problem statement which will guide their research. In addition, they conduct a preliminary literature review to develop the rationale for their research. (3 credits)</i></p> <p>DELIVERABLE: Research Rationale (Chapter 1).</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To identify the problem to be addressed by the field research study. • To conduct a preliminary review of literature to substantiate that the problem has relevance beyond the research site. • To establish the rationale and research objective(s) for conducting the proposed research. • To formulate a final business problem and research question.
	<i>RES9120 Review and Synthesis of Prior Research</i>
	<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>DELIVERABLE: Literature Review and Synthesis (Chapter 2)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To conduct a review of empirical research with respect to the proposed research topic. • To synthesize the findings of the reviewed literature to serve as the theoretical foundation and conceptual model for the proposed research. • To articulate the final research question and the justification for the proposed research. • To identify all variables (dependent, independent, parameters) relevant to the proposed research. • To formulate hypotheses relevant to the proposed research.
	<i>RES9130 Proposed Research Methodology</i>
	<p><i>In this course, students develop a methodology using hypothesis-testing. In addition, they evaluate the feasibility of standard research design types within the context of the proposed research site and document resource requirements for the proposed project in the Proposed Research Plan (PRP) as the final deliverable in this course. (3 credits)</i></p> <p>DELIVERABLE: Proposed Research Plan (PRP) (Chapters 1, 2, and 3.1 through 3.4)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To summarize the research hypotheses for the proposed research. • To develop conceptual definitions of study variables. • To define operational measures of study variables. • To identify the context of the study including setting, population and sample.
Step 5	Attaining Doctoral Candidacy Status
	<i>Submission of the PRP</i>
	<p><i>Upon approval of the Dean of Doctoral Research, students submit the PRP to the Candidacy Committee. If approved, students achieve Candidacy status and may begin to develop the Research Design Specification (RDS).</i></p> <p>OBJECTIVE:</p> <ul style="list-style-type: none"> • To obtain Candidacy.

PHASE III	PLANNING THE RESEARCH
Step 6	Developing the Data Collection Plan
	<p><i>RES9140 Research Design: Data Collection Plan</i></p> <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>DELIVERABLE: Research Design, Data Collection Plan (Chapter 3.5 through 3.6)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To specify the methods to be used to measure each variable. • To identify or produce reliable, valid instrument(s) for use in data collection. • To specify the detailed data collection procedures to be used. • To conduct a pilot test of the selected instrument(s).
	<p><i>Obtaining IRB Approval</i></p> <p><i>Prior to the completion of the RDS, doctoral candidates must submit the IRB Research Application for IRB approval. (See Appendix C.)</i></p>
Step 7	Developing the Research Design Specification (RDS)
	<p><i>RES9150 Research Design: Results and Findings</i></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>DELIVERABLE: Data Analysis Plan (Chapter 4.1)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To specify the methods to be used to analyze the relationships between the independent variables and the dependent variable leading to hypothesis testing.
	<p><i>RES9160 Research Design Specification</i></p> <p><i>In this course, students finalize the operational requirements of the proposed research study. (3 credits)</i></p> <p>DELIVERABLE: Research Design Specification (RDS) (Chapters 1, 2, 3, and 4.1)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To integrate all previous work into the final specifications of the research design. • To obtain IRB approval of the Data Collection Plan and instruments. • To understand copyright requirements of a published research study.
Step 8	Obtaining Approval to Conduct Research
	<p><i>Upon approval of the Dean of Doctoral Research, doctoral candidates submit the RDS to the Candidacy Committee for approval to conduct research. After the RDS is approved, the Dissertation Committee is appointed.</i></p> <p>OBJECTIVE:</p> <ul style="list-style-type: none"> • To obtain approval of the RDS • To gain authorization to conduct research.

PHASE IV	COMPLETING THE DISSERTATION
Step 9	Implementing the Research Plan and Documenting Research Findings
	<i>DST9310 Data Collection and Preparation</i> <i>In this course, doctoral candidates implement the approved research design by collecting data and preparing data for analysis, including cleaning the data set, providing data variable names and coding. (2-6 credits)</i> DELIVERABLE: Results and Findings (Chapter 4.2 through 4.3)
	<i>DST9320 Data Analysis and Findings</i> <i>In this course, doctoral candidates implement the approved data analysis plan and review findings with advisors. (1-2 credits)</i> DELIVERABLE: Dissertation (Chapters 1, 2, 3, 4, and 5)
	<i>DST9325 Continuing Dissertation Development (If Required)</i> <i>Doctoral candidates requiring additional time to produce an approved dissertation, enroll in this course to receive continued advising. Candidates may repeat the course until the dissertation is approved for defense. (1 credit)</i>
Step 10	Obtaining Approval to Defend
	<i>Doctoral candidates submit a final draft of the dissertation document to the Chair for approval to be submitted for Quality Review (APA format, adherence to guidelines and quality criteria). Once the document passes Quality Review, the Chair forwards the document to the Dissertation Committee and the Dean of Doctoral Research for Approval to Defend. Upon approval, the defense is scheduled.</i> OBJECTIVE: <ul style="list-style-type: none"> To obtain approval to defend the dissertation.
PHASE V	OBTAINING DISSERTATION APPROVAL
Step 11	Presenting Dissertation Findings
	<i>DST9330 Dissertation Documentation and Defense</i> <i>In this course, candidates present their findings to the Dissertation Committee at the defense. (1 credit)</i>
Step 12	Obtaining Final Approval of Dissertation
	<i>At the defense, doctoral candidates present their findings and respond to questions posed by the Chief Academic Officer, the Dean of Doctoral Research, Dissertation Committee members and invited faculty.</i> OBJECTIVE: <ul style="list-style-type: none"> To obtain final approval of the dissertation.
PHASE VI	PUBLISHING THE DISSERTATION