

CURRICULUM OVERVIEW

DOCTORATE 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 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 practitioners.
- To demonstrate integration of the core concepts of risk analysis, project planning, and change management through the completion of the Qualifying Exams.
- To demonstrate mastery of literature-based research skills and APA documentation and citation formats through the completion of Level I Comprehensive Exams.
- To develop primary field research competencies that can result in a contribution to knowledge in a specialized field of study relevant to Information Assurance practitioners.
- To contribute new Information Assurance knowledge by conducting application- or problem-driven research which extends prior empirically developed research.

Learning Outcomes

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

- 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 methodologies and analysis techniques in conducting primary field research in a specialized area of Information Assurance.
- Contribute to the body of knowledge through the documentation of field 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 DIA program must pass the Qualifying Exam. This exam consists of a 20-25 page Strategic Risk Mitigation Plan which integrates principles and techniques of risk analysis, project planning, and change management. This exam is the required deliverable for the IA9200 course.

Comprehensive Exams (Level I)

Doctoral students enrolled in the DIA program must pass Level I Comprehensive Exams. Level I Comprehensive Exams consist of three 25-30 page research papers which are produced in courses IA8220, IA8230 and IA8240. These exams must demonstrate mastery of the content and literature-based research skills, while utilizing APA format and citation requirements. If necessary, students may repeat any or all of the Level I Comprehensive Exams.

Credit Requirements

The *Doctorate in Information Assurance* consists of a minimum of 64 semester credits beyond a Master's degree, including 24 credits of core courses, 9 credits of comprehensive exam courses, 27 credits of research-preparation courses and 4 credits of dissertation development courses. Students must pass Comprehensive Exams prior to beginning research-related courses.

Specialization Option

DIA 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 76. 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	<p data-bbox="310 247 1146 275"><i>IA7020 Information Security Systems and Organizational Awareness</i></p> <p data-bbox="310 281 1430 369"><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 data-bbox="310 375 792 403">DELIVERABLES: Best Practice Analyses</p> <p data-bbox="310 409 607 436">COURSE OBJECTIVES:</p> <ul data-bbox="321 438 1425 743" style="list-style-type: none"> <li data-bbox="321 438 1344 495">• To compare and contrast the mechanisms and procedures used by management to influence behavior, use, and content of an information system. <li data-bbox="321 501 1409 558">• To propose best practices which utilize the means and methods of disguising information through cryptography in order to protect confidentiality and integrity. <li data-bbox="321 564 1333 621">• To evaluate the impact of high level procedures, structures and standards used in defining, designing, and implementing information systems and technology. <li data-bbox="321 627 1403 684">• To analyze structures, transmission methods, transport formats and security measures that enable confidentiality, integrity and availability in business communications. <li data-bbox="321 690 1425 743">• To assess best practices used in establishing controls, within business applications, that support the security strategy of the enterprise.
2	<p data-bbox="310 751 1036 779"><i>IA7030 Legal and Ethical Practices in Information Security</i></p> <p data-bbox="310 785 1438 873"><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 data-bbox="310 879 792 907">DELIVERABLES: Best Practice Analyses</p> <p data-bbox="310 913 607 940">COURSE OBJECTIVES:</p> <ul data-bbox="321 942 1406 1220" style="list-style-type: none"> <li data-bbox="321 942 1382 999">• To assess associated security risks of various frameworks, policies, and structures of enterprise information assets. <li data-bbox="321 1005 1406 1062">• To evaluate physical, procedural, and environmental risks associated with a business information technology infrastructure. <li data-bbox="321 1068 1382 1125">• To recommend procedures and best practices required to preserve business in the face of major disruptions to normal operations. <li data-bbox="321 1131 1357 1159">• To propose best practices for the protection and control of information technology resources. <li data-bbox="321 1165 1406 1220">• 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	<p data-bbox="310 1228 1008 1255"><i>IA7040 Information Security and Organizational Change</i></p> <p data-bbox="310 1262 1443 1377"><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 data-bbox="310 1383 824 1411">DELIVERABLE: Change Management Plan</p> <p data-bbox="310 1417 607 1444">COURSE OBJECTIVES:</p> <ul data-bbox="321 1446 1390 1656" style="list-style-type: none"> <li data-bbox="321 1446 1312 1503">• To analyze the factors influencing the need for change and the imperatives for managing information security change initiatives in the workplace. <li data-bbox="321 1509 1328 1566">• To evaluate the need for a specific Information Security change initiative at the group and organizational level. <li data-bbox="321 1572 1312 1600">• To evaluate how the proposed change aligns with corporate leadership goals and culture. <li data-bbox="321 1606 1276 1633">• To develop a change strategy and identify potential resistance factors to be managed. <li data-bbox="321 1640 1390 1656">• To apply appropriate models to implement a sustainable Information Security change initiative.

4	<i>RM8250 Web-Based Research Methods in Information Security</i>
	<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	<i>RM6000 Effective Writing in Information Security Analysis</i>
	<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>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	<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.
7	<i>PM8100 Information Security Project Management</i>
	<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 (Qualifying Exam)</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>IA8220 Security Program Strategies and Implementation (Comprehensive Exam-Level I)</i>
	<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.
10	<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.
11	<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.

PHASE I	IDENTIFYING A DISSERTATION TOPIC
Step 1	Understanding the Research Process
	<p><i>Orientation to the University of Fairfax Dissertation Process</i></p> <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.
	<p><i>RM9300 Applying the Research Paradigm to Information Security</i></p> <p><i>In this course, students utilize a published research study as a model to review and analyze the research paradigm and the components of empirical research. (3 credits)</i></p> <p>DELIVERABLE: Analysis of research design components.</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.
	<p><i>RES9100 Feasible Problem-Driven Research in Information Security</i></p> <p><i>In this course, students apply the concept of problem-driven research in order to identify feasible topic areas for their field research study. Students also identify a research site and utilize problems occurring there as a basis for selecting a researchable (feasible, non-trivial) research topic. Finally, they identify the dependent variable to be studied. (3 credits)</i></p> <p>DELIVERABLES: Research Project Feasibility Analysis;</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.
Step 2	Understanding Research Principles and Techniques
	<p><i>RM8250 Web-Based Research Methods in Information Security</i></p> <ul style="list-style-type: none"> Completed in sequence #4
	<p><i>RM6000 Effective Writing in Information Security Analysis</i></p> <ul style="list-style-type: none"> Completed in sequence #5
	<p><i>RM9100 Qualitative and Quantitative Analysis</i></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>DELIVERABLES: Methodology Critique; 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.

Step 3	Obtaining Approval for a Feasible Problem-Driven Research Topic
	<i>Dissertation Bootcamp - Presentation of Dissertation Topic</i>
	<i>Students present their topic selections and feasibility analyses to the Program Director and invited faculty. This presentation includes the context of the study, the feasibility of the research site, and the topic to be researched. If the topic is approved, a Dissertation Committee Chair is appointed prior to the start of the next course.</i>
	BOOTCAMP OBJECTIVE:
	<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>
	<i>In this course, students articulate the problem statement and conduct a preliminary research literature review in Information Security to develop the rationale for their research. In addition, students identify and review other relevant bodies of research to be examined. (3 credits)</i>
	DELIVERABLE: Research Rationale (Chapter 1).
	COURSE OBJECTIVES:
	<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 preliminary research question.
	<i>RES9120 Review and Synthesis of Prior Research</i>
	<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>
	DELIVERABLE: Literature Review and Synthesis (Chapter 2)
	COURSE OBJECTIVES:
	<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 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 identify hypotheses relevant to the proposed research.
	<i>RES9130 Information Security Research Design: Theory and Methodology</i>
	<i>In this course, students define the theoretical framework and select a research design approach (exploratory or 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 research project. (3 credits)</i>
	DELIVERABLE: Proposed Research Plan (PRP) (Chapters 1, 2, and 3.1 through 3.4)
	COURSE OBJECTIVES:
	<ul style="list-style-type: none"> • To define the theoretical framework for the proposed research. • To evaluate and select the appropriate approach to the research (exploratory or hypothesis-testing). • To select at least one feasible design type that can be implemented at the proposed research site. • To identify a research hypothesis and assess the plausibility of rival hypotheses (if applicable to the research design). • To identify the context of the study including setting, population and sample. • To document the project resource requirements for the proposed research (people, cost, time, materials, support services).

Step 5	Attaining Doctoral Candidacy Status
	<i>Submission of the PRP</i> <i>Upon approval of their Chair, 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>
	OBJECTIVE: <ul style="list-style-type: none"> To obtain Candidacy.
PHASE III	PLANNING THE RESEARCH
Step 6	Developing the Data Collection Plan
	<i>RES9140 Information Security Research Design: Data Collection Plan</i> <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>
	DELIVERABLE: Data Collection Plan (Chapters 3.5.1 through 3.5.5) COURSE OBJECTIVES: <ul style="list-style-type: none"> To describe how the context of the study will affect data collection. 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). To develop appropriate displays of data including charts, tables and graphs using illustrative data.
Step 7	Developing the Data Analysis Plan
	<i>RES9150 Information Security Research Design: Data Analysis Plan</i> <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>
	DELIVERABLE: Data Analysis Plan (Chapters 4.1 through 4.2) COURSE OBJECTIVES: <ul style="list-style-type: none"> To describe how the context of the study will affect data analysis. To specify the methods to be used to analyze the relationships among the variables. To identify appropriate analytical methods to be used to generate or test the hypothesis. To specify the detailed data analysis procedures to be used. To develop appropriate displays of results using illustrative data.
Step 8	Obtaining IRB Approval
	<i>Prior to the completion of the RDS, doctoral candidates must submit the IRB Research Application to the IRB for approval.</i>
Step 9	Developing the Research Design Specification (RDS)
	<i>RES9160 Research Design Specification</i> <i>In this course, students finalize the operational requirements of the proposed research study. (3 credits)</i>
	DELIVERABLE: Research Design Specification (RDS) COURSE OBJECTIVES: <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 10	Obtaining Approval to Conduct Research
	<i>Upon approval of their Chair, doctoral candidates submit the RDS to the Candidacy Committee, to demonstrate readiness to conduct research. After the RDS is approved, the Dissertation Committee is appointed.</i> OBJECTIVE: <ul style="list-style-type: none"> To obtain approval of the RDS To gain authorization to conduct research.

PHASE IV	COMPLETING THE DISSERTATION
Step 11	Implementing the Research Plan
	<i>DST9200 Data Collection and Analysis</i>
	<i>In this course, doctoral candidates implement the approved research design by collecting and analyzing data. (2-6 credits)</i>
	<i>DST9205 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. (2 credits)</i>
Step 12	Documenting the Research Findings
	<i>DST9210 Dissertation Documentation and Defense</i>
	<i>In this course, candidates produce and submit the final draft of the dissertation for approval. (2-6 credits)</i>
PHASE V	OBTAINING DISSERTATION APPROVAL
Step 13	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 Program Director 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.
Step 14	Obtaining Final Approval of Dissertation
	<i>At the defense, doctoral candidates present their findings and respond to questions posed by Dissertation Committee members.</i>
	OBJECTIVE:
	<ul style="list-style-type: none"> To obtain final approval of the dissertation.
PHASE VI	PUBLISHING THE DISSERTATION