

CURRICULUM OVERVIEW

DOCTOR OF SCIENCE IN INFORMATION ASSURANCE¹

Description

This degree program helps students to advance in cybersecurity policy development and research positions. In this program, students engage in primary research and complete original applied field research, derived from theory and practice, which contributes to the advancement of knowledge and application in Information Assurance.

This program fosters the development of students who:

- Are recognized as thought leaders with expertise in a specialized field of applied research relevant to the cybersecurity community
- Apply critical thinking and problem-solving skills in assessing research issues relevant to information assurance
- Possess an awareness and expertise in recognizing gaps in knowledge that have generalized applicability to the cybersecurity community
- Have a commitment to advancing the state of practice and knowledge relevant to the field of information assurance
- contribute to the strategic development of practices in the field of cybersecurity

Program Objectives

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

- Demonstrate primary research competencies through the completion of an original applied field research project in information assurance
- Demonstrate secondary research competencies in the investigation and identification of research topics relevant to information assurance practitioners
- Analyze, evaluate and propose opportunities for applied research projects relevant to the cybersecurity community
- Formulate the rationale and justification for conducting primary research which investigates practice-relevant research questions
- Apply appropriate hypothesis testing methodologies and analysis techniques in conducting practice-driven primary research
- Interpret and apply the results and findings from individual primary research projects in the formulation of recommendations to industry practitioners

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, is used to evaluate mastery of the concepts and foundations of applied research and is administered at the conclusion of the RM8500 course.

Comprehensive Exams (Level I and II)

Doctoral students enrolled in the DSc program must pass two Level I Comprehensive Exams completed in CEX8220, CEX8230 or CEX8240. Each Level I Comprehensive Exam consists of a 25-30 page research paper on a specified topic in Information Security and must demonstrate mastery of content and literature-based research skills, while utilizing APA format and citation requirements.

DSc students must also pass the Level II Comprehensive Exam completed in CEX9200, which consists of a 25-30 page paper addressing a research question relating to one of the 10 Information Security domains known as the Common Body of Knowledge (CBK). The exam 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 63 credits of pre-dissertation courses (18 credits of Information Security content taken from core and specialization courses, 18 credits of research methods courses, 9 credits of comprehensive exam courses, 18 credits of research-preparation courses) and 7 credits of dissertation development courses.

Earning Graduate Certificates

DSc candidates complete the requirements for graduate certificates as they progress through their programs. Upon completion of the required courses, they may elect to receive the applicable graduate certificate(s) listed in the catalog under the *Graduate Certificate Program*.

COURSES, OBJECTIVES AND DELIVERABLES

PRE-DISSERTATION COURSEWORK

IA7020 Information Security Systems and Organizational Awareness

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)

DELIVERABLES: Best Practice Analyses

COURSE OBJECTIVES:

- To analyze structures, transmission methods, transport formats and security measures that enable confidentiality, integrity and availability in business communications.
- To examine best practices which serve to manage and reduce security risks associated with various frameworks, networks and technology structures of an enterprise.
- To assess best practices used in establishing controls, within business applications, which support the security strategy of an enterprise.
- To evaluate the impact of high level procedures, structures and standards used in defining, designing, and implementing information systems and technology.
- To propose best practices which utilize the means and methods of disguising information through cryptography in order to protect confidentiality and integrity of data.

IA7030 Legal and Ethical Practices in Information Security

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)

DELIVERABLES: Best Practice Analyses

COURSE OBJECTIVES:

- 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.

IA8010 Business and Security Risk Analysis

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)

DELIVERABLES: Business Risk Assessment Report

COURSE OBJECTIVES:

- 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.

IA8020 Security Policies, Standards and Procedures

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)

DELIVERABLES: Enterprise Security Critique; Security Governance Report

COURSE OBJECTIVES:

- 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.

IA8030 Design, Development and Evaluation of Security Controls

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)

DELIVERABLES: General IT Controls Review; Application Controls Review

COURSE OBJECTIVES:

- 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.

IA8190 Forensic Evaluation and Incident Response Management

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)

DELIVERABLE: Forensic Evaluations; Incident Response Plan

COURSE OBJECTIVES:

- 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.

RM8250 Web-Based Research Methods in Information Security

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)

DELIVERABLES: Comparative Analysis of Sources; Annotated Bibliography

COURSE OBJECTIVES:

- 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.

RM6000 Effective Writing in Information Security Analysis (Qualifying Exam)

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)

DELIVERABLE: Annotated Bibliography; Best Practice Research Recommendation

COURSE OBJECTIVES:

- To demonstrate effective written and oral communication skills.
- To demonstrate knowledge of the secondary research process.
- To formulate a rationale for applied research in Information Security based on review of current literature.
- To demonstrate knowledge of APA requirements for format, source identification and citations in research writing.

RM8500 Research Foundations for the InfoSec Practitioner

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)

DELIVERABLE: Research Practice Sets

COURSE OBJECTIVES:

- To understand the research paradigm and how it applies to the field research process
- To assess what constitutes a non-trivial and feasible research problem
- To formulate appropriate research questions for field research studies
- To distinguish the characteristics of dependent and independent variables
- To construct testable hypotheses appropriate for field research

COMPREHENSIVE EXAMS – LEVEL I (two of the following)

CEX8220 Security Program Strategies and Implementation (Level 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)

DELIVERABLES: Security Program Review; Research Paper

COURSE OBJECTIVES:

- 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.

CEX8230 Legal and Ethical Management Issues in Information Security (Level 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)

DELIVERABLES: Regulatory Analysis; Research Paper

COURSE OBJECTIVES:

- 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.

CEX8240 Strategic and Technological Trends in Information Security (Level 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)

DELIVERABLES: Technology Review; Research Paper

COURSE OBJECTIVES:

- 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.

COMPREHENSIVE EXAMS – LEVEL II

CEX9200 Research Topics in Information Security (Level II)

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)

DELIVERABLES: Research Paper

COURSE OBJECTIVES:

- 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.

DISSERTATION PROJECT PLAN:

PHASE I: IDENTIFYING A DISSERTATION TOPIC

Step 1: Understanding the Dissertation Research Process

Dissertation Project Plan Orientation

During this video orientation, students review of the Dissertation Handbook, deliverable requirements, and the approval process for dissertation deliverables.

ORIENTATION OBJECTIVE:

- 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

RM9100 Qualitative and Quantitative Analysis

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)

DELIVERABLES: Questionnaire Quality Assessment; Data Collection and Analysis Report

COURSE OBJECTIVES:

- 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: Identifying a Feasible and Accessible Research Site
<i>RM9150 Feasible Problem-Driven Research in Information Security</i>
<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>
DELIVERABLES: Research Site Access Plan
COURSE OBJECTIVES:
<ul style="list-style-type: none"> • To understand what constitutes an acceptable research site. • To select 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.
<i>RM9250 Building a Knowledge-Base in the Information Security Discipline</i>
<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>
DELIVERABLE: Research Project Feasibility Analysis
COURSE OBJECTIVES:
<ul style="list-style-type: none"> • To identify potential problems affecting the research population. • To recognize potential dependent variables that can be studied. • To formulate an acceptable research question applicable to the problem being studied. • To articulate a problem statement that will be addressed by the proposed study. • To select a researchable topic area (site, problem, Information Security domain).
Step 4: 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 Dean of Doctoral Research and invited faculty. This presentation includes the context of the study, the feasibility of the research site, and a proposed topic area to be researched. If the topic is approved, a Dissertation Advisor 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 Advisor.
PHASE II: ACHIEVING CANDIDACY
Step 5: Developing the Proposed Research Plan (PRP)
<i>RES8510 Research Topic Rationale</i>
<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>
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 objectives for conducting the proposed research. • To formulate an appropriate research question to guide the proposed study.

RES8520 Review and Synthesis of Prior Research

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)

DELIVERABLE: Literature Review and Synthesis (Chapter 2)

COURSE OBJECTIVES:

- To conduct a review of empirical research with respect to the proposed research topic.
- To identify all variables (dependent, independent, parameters) relevant to the proposed research.
- To formulate hypotheses relevant to the proposed research.
- To synthesize the findings of the reviewed literature to serve as the theoretical foundation for the proposed research.
- To construct a conceptual model which describes the relationships among and between the study variables.
- To articulate the final research question and the justification for the proposed research.

RES8530 Proposed Research Methodology

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)

DELIVERABLE: Proposed Research Plan (PRP) (Chapters 1, 2, and 3.1 through 3.4)

COURSE OBJECTIVES:

- To define operational measures of study variables.
- To describe the context of the study including setting, population and sample.
- To identify and justify the design approach of the study (qualitative vs. quantitative; exploratory vs. hypothesis-testing)

RES8540 Continuing PRP Development

Doctoral students requiring additional time to produce an approved Proposed Research Plan (PRP) enroll in this course until the document is approved by the Candidacy Committee. (1 credits)

DELIVERABLE: Proposed Research Plan (PRP) (Chapters 1, 2, and 3.1 through 3.4)

Step 6: Attaining Doctoral Candidacy Status**Submission of the PRP**

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).

OBJECTIVE:

- To obtain Candidacy.

PHASE III: PLANNING THE RESEARCH**Step 7: Developing the Research Design Specification (RDS)****RES8550 Research Design: Data Collection Plan**

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)

DELIVERABLE: Research Design, Data Collection Plan (Chapter 3.5 through 3.6)

COURSE OBJECTIVES:

- To specify the design of the study using an established model.
- To identify or produce reliable, valid instrument(s) for use in data collection.
- To specify the detailed data collection procedures to be used.
- To describe the pilot test of the selected instrument(s).

<p>RES8560 Research Design: Results and Findings</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 in analysis of the data. • To explain the rationale of the selection of the identified methods of analysis. • To describe the treatment for missing data.
<p>RES8570 Research Design Specification</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>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.
<p>RES8580 Continuing RDS Development</p> <p><i>Doctoral students requiring additional time to produce an approved Research Design Specification (RDS) enroll in this course until the document is approved by the Candidacy Committee. (1 credits)</i></p> <p>DELIVERABLE: Research Design Specification (RDS) (Chapters 1, 2, 3, and 4.1)</p>
<p>Step 8: Obtaining Approval to Conduct Research</p>
<p>Submission of the RDS</p> <p><i>Upon approval of the Dean of Doctoral Research, doctoral candidates submit the RDS to the Candidacy Committee. In addition to the RDS, doctoral candidates must submit the IRB Research Application for IRB approval. If the Candidacy Committee approves both, the Dissertation Committee and Committee Chair are appointed and students are granted approval to conduct research.</i></p> <p>OBJECTIVE:</p> <ul style="list-style-type: none"> • To obtain IRB Approval. • To obtain approval of the RDS. • To have a Dissertation Committee and Committee Chair appointed. • To gain authorization to conduct research.
<p>PHASE IV: CONDUCTING THE RESEARCH</p>
<p>Step 9: Implementing the Research Plan and Documenting Research Findings</p>
<p>DST8510 Data Collection and Preparation</p> <p><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. (1-6 credits)</i></p> <p>DELIVERABLE: Data Collection Methods (Chapter 3.6 revisions)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To collect data from the identified research subjects following procedures identified in the approved RDS. • To document methods and procedures performed.
<p>DST8520 Data Analysis and Findings</p> <p><i>In this course, doctoral candidates implement the approved data analysis plan and review findings with advisors. (1-6 credits)</i></p> <p>DELIVERABLE: Results and Findings (Chapter 4.2 through 4.3)</p> <p>COURSE OBJECTIVES:</p> <ul style="list-style-type: none"> • To analyze the data collected using the analysis methods identified in the approved RDS. • To draw conclusions and identify implications from the findings. • To document the procedures, analyses, findings and conclusions.
<p>DST8530 Continuing Dissertation Development (If Required)</p> <p><i>Doctoral candidates requiring additional time to produce an approved dissertation enroll in this course until the dissertation is approved for defense. (1 credit)</i></p>

Step 10: Obtaining Approval to Defend

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.

OBJECTIVE:

- To obtain approval to defend the dissertation.
- To meet the standards of the Quality Review.

PHASE V: OBTAINING DISSERTATION APPROVAL**Step 11: Defending the Dissertation*****DST8540 Dissertation Documentation and Defense***

In this course, candidates present their findings to the Dissertation Committee at the defense. (1-3 credits)

DELIVERABLE: Oral Dissertation Defense**COURSE OBJECTIVES:**

- To articulate a thorough understanding of the study conducted: topic, analyses, findings and conclusions.

Step 12: Obtaining Final Approval of the Dissertation

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.

OBJECTIVE:

- To obtain final approval of the dissertation.

PHASE VI: PUBLISHING THE DISSERTATION

After final approval of the defense, the Dissertation Committee Chairperson and the Dean of Doctoral Research sign the approval page that is incorporated into the final document. The document is prepared for printing and binding. Once copy is retained by the University, and one copy is provided to the Dissertation Chairperson. Students may order as many copies of the bound document as they wish for personal use.