



Curriculum Overview

2011

**2070 Chain Bridge Road
Suite G-100
Vienna, Virginia 22182**

**703.790.3200
www.UFairfax.net**

Table of Contents

CURRICULA	2
Doctorate in Information Assurance (DIA)	2
Doctor of Science (DSc) in Information Assurance.....	3
Master of Science in Information Security Management (MSISM).....	4
Master of Science in Enterprise Management (MSEM)	6
Graduate Certificates	7
COURSE DESCRIPTIONS	10
Core Courses	10
Specialization Courses	12
Research Courses	13
Elective Courses	16
Professional Development Courses	16

CURRICULA

Doctorate in Information Assurance (DIA)

<i>Course #</i>	<i>Course Title</i>
-----------------	---------------------

Core Courses:

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA7040	<i>Information Security and Organizational Change</i>
IA8010	<i>Business and Security Risk Analysis</i>
PM8100	<i>Information Security Project Management</i>
IA9200	<i>Strategic Analysis in Information Security</i>

Specialization Courses:

IA8020	<i>Security Policies, Practices and Standards</i>
IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>

Comprehensive Exam Courses:(two of the following)

IA8220	<i>Security Program Strategies and Implementation (Comprehensive Exam-Level I)</i>
IA8230	<i>Legal and Ethical Management Issues in Information Security (Comprehensive Exam-Level I)</i>
IA8240	<i>Strategic and Technological Trends in Information Security (Comprehensive Exam-Level I)</i>

Research Methods Courses:

RM6000	<i>Effective Writing in Information Security Analysis (Qualifying Exam)</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>
RM9100 ¹	<i>Qualitative and Quantitative Analysis</i>
RM9150	<i>Feasible Problem-Driven Research in Information Security</i>
RM9200	<i>Applying the Design Research Paradigm to Information Security</i>

Research Preparation Courses:

RES8110	<i>Research Needs and Requirements Analysis</i>
RES8120	<i>Review of Prior Research and Methodology</i>
RES8130	<i>Operational Design and Specification</i>

Dissertation Development Courses:

DST9100	<i>Integration and Implementation Feasibility Testing and Planning</i>
DST9205 ²	<i>Continuing Dissertation Development</i>
DST9210	<i>Dissertation Documentation and Defense</i>

Minimum credits required for DIA: 60

¹ Comprehensive Exams must be completed and passed prior to enrollment in this course.

² This course must be repeated until deliverables are approved.

Doctor of Science (DSc) in Information Assurance

Course # Course Title

Core Courses:

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA8010	<i>Business and Security Risk Analysis</i>
IA9200	<i>Strategic Analysis in Information Security</i>

Specialization Courses:

IA8020	<i>Security Policies, Practices and Standards</i>
IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>

Comprehensive Exam Courses:

IA8220	<i>Security Program Strategies and Implementation (Comprehensive Exam-Level I)</i>
IA8230	<i>Legal and Ethical Management Issues in Information Security (Comprehensive Exam-Level I)</i>
IA8240	<i>Strategic and Technological Trends in Information Security (Comprehensive Exam-Level I)</i>
CEX9100	<i>Comprehensive Exams Level II</i>

Research Methods Courses:

RM6000	<i>Effective Writing in Information Security Analysis (Qualifying Exam)</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>
RM9100 ³	<i>Qualitative and Quantitative Analysis</i>
RES9150	<i>Feasible Problem-Driven Research in Information Security</i>
RM9300	<i>Applying the Empirical Research Paradigm to Information Security</i>

Research Preparation Courses:

RES9110	<i>Research Topic Rationale</i>
RES9120	<i>Review and Synthesis of Prior Research</i>
RES9130	<i>Proposed Research Methodology</i>
RES9140	<i>Research Design: Data Collection Plan</i>
RES9150	<i>Research Design: Results and Findings</i>
RES9160	<i>Research Design Specification</i>

Dissertation Development Courses:

DST9310	<i>Data Collection and Preparation</i>
DST9320	<i>Data Analysis and Findings</i>
DST9325 ⁴	<i>Continuing Dissertation Development</i>
DST9330	<i>Dissertation Documentation and Defense</i>

Minimum credits required for DSc: 70

³ Comprehensive Exams must be completed and passed prior to enrollment in this course.

⁴ This course must be repeated until deliverables are approved.

Master of Science in Information Security Management (MSISM)

Specialization: Information Security Analysis (ISA)

Course # Course Title

Core Courses:

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA7040	<i>Information Security and Organizational Change</i>
IA8010	<i>Business and Security Risk Analysis</i>
PM8100	<i>Information Security Project Management</i>
IA9200	<i>Strategic Analysis in Information Security</i>

Research Methods Courses:

RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>

Specialization Courses:

IA8120	<i>Information Security Policy Planning and Analysis</i>
IA8020	<i>Security Policies Standards and Procedures</i>
IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>

Credits required for MSISM: 36

Specialization: Information Security Auditing (IAU)

Course # Course Title

Core Courses:

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA7040	<i>Information Security and Organizational Change</i>
IA8010	<i>Business and Security Risk Analysis</i>
PM8100	<i>Information Security Project Management</i>
IA9200	<i>Strategic Analysis in Information Security</i>

Research Methods Courses:

RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>

Specialization Courses:

IA8050	<i>Security Risk and Vulnerability Assessment</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>
IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8110	<i>Certification and Accreditation</i>

Credits required for MSISM: 36

Specialization: Information System Certification (ISC)

Course # Course Title

Core Courses:

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA7040	<i>Information Security and Organizational Change</i>
IA8010	<i>Business and Security Risk Analysis</i>
PM8100	<i>Information Security Project Management</i>
IA9200	<i>Strategic Analysis in Information Security</i>

Research Methods Courses:

RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>

Specialization Courses:

IA8020	<i>Security Policies Standards and Procedures</i>
IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8070	<i>Design and Development of Security Architectures</i>
IA8110	<i>Certification and Accreditation</i>

Credits required for MSISM: 36

Specialization: Information Security Engineering (ISE)

Course # Course Title

Core Courses:

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA7040	<i>Information Security and Organizational Change</i>
IA8010	<i>Business and Security Risk Analysis</i>
PM8100	<i>Information Security Project Management</i>
IA9200	<i>Strategic Analysis in Information Security</i>

Research Methods Courses:

RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>

Specialization Courses:

IA8050	<i>Security Risk and Vulnerability Assessment</i>
IA8060	<i>Intrusion Detection, Attacks and Countermeasures</i>
IA8070	<i>Design and Development of Security Architectures</i>
IA8080	<i>Security Solution Implementation</i>

Credits required for MSISM: 36

Master of Science in Enterprise Management (MSEM)

Specialization: Information Security Analysis (ISA)

Course # Course Title

Core Courses:

EM7020	<i>Organizational Behavior and Awareness</i>
EM7030	<i>Legal and Ethical Practices</i>
EM7040	<i>Organizational Change</i>
EM6000	<i>Effective Writing</i>
EM8250	<i>Web-Based Research Methods</i>
EM8010	<i>Business Risk Analysis</i>
EM8100	<i>Project Management</i>
EM9200	<i>Strategic Analysis</i>

Specialization Courses:

IA8120	<i>Information Security Policy Planning and Analysis</i>
IA8020	<i>Security Policies Standards and Procedures</i>
IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>

Credits required for MSEM: 36

Graduate Certificates

CISSP Best Practices (CBP)⁵

Course # Course Title

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IC7000	<i>(ISC)² Official CISSP Review Seminar</i>

Credits required for Certificate: 6

NSA 4011 Information Systems Security Professional (ISSP)⁶

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA8010	<i>Business and Security Risk Analysis</i>
IA8020	<i>Security Policies, Standards and Procedures</i>
IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>

Credits required for Certificate: 18

NSA 4012 Senior Systems Manager (SSM)⁷

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA8010	<i>Business and Security Risk Analysis</i>
IA8020	<i>Security Policies, Standards and Procedures</i>
IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>

Credits required for Certificate: 18

Designing Empirically-Based Research for Information Security Practitioners (DEBR)

RES9110	<i>Research Topic Rationale</i>
RES9120	<i>Review and Synthesis of Prior Research</i>
RES9130	<i>Proposed Research Methodology</i>
RES9140	<i>Research Design: Data Collection Plan</i>
RES9150	<i>Research Design: Results and Findings</i>
RES9160	<i>Research Design Specification</i>

Credits required for Certificate: 18

⁵ This certificate requires the student to provide verification of attendance at an (ISC)² Official CISSP Review Seminar.

⁶ Upon completion of this certificate the student is awarded the NSA 4011 Certification for Information Systems Security Professionals (CNSS No.4011).

⁷ Upon completion of this certificate the student is awarded the NSA 4012 Certification for Senior Systems Managers (CNSS No.4012).

Designing Solution-Based Research for Information Security Practitioners (DSBR)

RES8110 *Research Needs and Requirements Analysis*

RES8120 *Review of Prior Research and Methodology*

RES8130 *Operational Design and Specification*

Credits required for Certificate: 9

Governance, Risk Management and Compliance (GRC)

Course # Course Title

IA8120 *Information Assurance Policy Planning and Analysis*

IA8020 *Security Policies Standards and Procedures*

IA8030 *Design, Development and Evaluation of Security Controls*

IA8210 *Risk Management and Compliance*

Credits required for Certificate: 12

Information Security Analysis (ISA)

IA8120 *Information Assurance Policy Planning and Analysis*

IA8020 *Security Policies Standards and Procedures*

IA8030 *Design, Development and Evaluation of Security Controls*

IA8190 *Forensic Evaluation and Incident Response Management*

Credits required for Certificate: 12

Information Security Auditing (IAU)

IA8050 *Security Risk and Vulnerability Assessment*

IA8190 *Forensic Evaluation and Incident Response Management*

IA8030 *Design, Development and Evaluation of Security Controls*

IA8110 *Certification and Accreditation*

Credits required for Certificate: 12

Information System Certification (ISC)

IA8020 *Security Policies Standards and Procedures*

IA8030 *Design, Development and Evaluation of Security Controls*

IA8070 *Design and Development of Security Architectures*

IA8110 *Certification and Accreditation*

Credits required for Certificate: 12

Information Security Engineering (ISE)

IA8050 *Security Risk and Vulnerability Assessment*

IA8060 *Intrusion Detection, Attacks and Countermeasures*

IA8070 *Design and Development of Security Architectures*

IA8080 *Security Solution Implementation*

Credits required for Certificate: 12

Information Security for the Enterprise (ISEN)

IA7020	<i>Information Security Systems and Organizational Behavior and Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA7040	<i>Information Security and Organizational Change</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>

Credits required for Certificate: 12

Information Security Research Practices (ISRP)

Course # Course Title

RM9100	<i>Qualitative and Quantitative Analysis</i>
RM9150	<i>Feasible Problem-Driven Research</i>

At least two of the following:

IA8220	<i>Security Program Strategies and Implementation</i>
IA8230	<i>Legal and Ethical Management Issues in Information Security</i>
IA8240	<i>Strategic and Technological Trends in Information Security</i>

At least one of the following:

RM9200	<i>Applying the Design Research Paradigm to Information Security</i>
RM9300	<i>Applying the Empirical Research Paradigm to Information Security</i>

Credits required for Certificate: 15 – 18

Strategic Implementation of Information Security in the Enterprise (SISE)

IA7040	<i>Information Security and Organizational Change</i>
IA9200	<i>Strategic Analysis in Information Security</i>
PM8100	<i>Information Security Project Management</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>
RM6000	<i>Effective Writing in Information Security Analysis</i>

Credits required for Certificate: 15

Strategic Analysis in Information Security (SAIS)

IA9200	<i>Strategic Analysis in Information Security</i>
RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>

Credits required for Certificate: 9

COURSE DESCRIPTIONS

CORE COURSES

Information Security Degrees

IA7020 Information Security Systems and Organizational Behavior and 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)*

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)*

IA7040 Information Security and Organizational Change

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)*

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)*

IA9200 Strategic Analysis in Information Security

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)*

PM8100 Information Security Project Management

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)*

Enterprise Management Degrees

EM6000 Effective Writing

In this course, students utilize secondary research to analyze a current best practice or process in an enterprise. Students write and present a position paper providing a rationale for research to evaluate the effectiveness of that practice or process. *(3 credits)*

EM7020 Organizational Behavior and Awareness

In this course, students critically analyze organizational behavior and awareness issues and evaluate best practices in implementing programs within the enterprise. *(3 credits)*

EM7030 Legal and Ethical Practices

In this course, students critically analyze ethical decision-making and evaluate the best practices employed in operations planning and management. *(3 credits)*

EM7040 Organizational Change

In this course, students analyze the principles of change management as they apply to the requirements and regulations of an enterprise. Students evaluate the factors which affect corporate decision-making when implementing enterprise-wide programs and the ability of the manager to translate corporate needs into projects. *(3 credits)*

EM8010 Business 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)*

EM8100 Project Management

In this course, students utilize PMI's Project Management Body of Knowledge (PMBOK) as a framework to apply project management concepts in the enterprise. Each student develops a project plan for a program assessment which incorporates the technical and behavioral characteristics of high performance teams. *(3 credits)*

EM8250 Web-Based Research Methods

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 the enterprise. 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)*

EM9200 Strategic Analysis

In this integrative course, students assess the 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)*

Prerequisite: EM7040, EM8010, EM8100

SPECIALIZATION COURSES

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)*

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)*

IA8050 Security Risk and Vulnerability Assessment

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)*

IA8060 Intrusion Detection, Attacks and Countermeasures

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)*

IA8070 Design and Development of Security Architectures

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)*

IA8080 Security Solution Implementation

In this course, students compare, contrast, and evaluate contemporary practices in the implementation of security solutions. *(3 credits)*

IA8110 Certification and Accreditation

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)*

IA8120 Information Assurance Policy Planning and Analysis

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)*

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)*

RESEARCH COURSES

Comprehensive Exam Courses

IA8220 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)

IA8230 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)

IA8240 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)

CEX9100 Comprehensive Exams Level II

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)

Research Methods Courses

RM6000 Effective Writing in Information Security Analysis

In this course, students utilize secondary research to analyze a current best practice or process in one of the 10 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. This paper serves as the Qualifying Exam for doctoral students. (3 credits)

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)

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)
Prerequisite: Comprehensive Exams

RM9150 Feasible Problem-Driven Research in Information Security

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)

RM9200 Applying the Design Research Paradigm to Information Security

In this course, doctoral students utilize the design 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)

RM9300 Applying the Empirical Research Paradigm to Information Security

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 variable to be studied. (3 credits)

Research Preparation Courses

RES8110 Research Needs and Requirements Analysis

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)

Prerequisite: RM9200

RES8120 Review of Prior Research and Methodology

In this course, students develop a conceptual model of the proposed research, conduct a literature review in Information Security and other relevant bodies of research and synthesize relevant empirical research in order to provide justification for their conceptual model. Students document the proposed project in the *Proposed Research Plan* (PRP) as the final deliverable in this course. (3 credits)

RES8130 Operational Design and Specification

In this course, students finalize the operational requirements of the proposed research study and specify their proposed improvement in professional practice. Students document protocols utilized in the proposed project in the *Protocol Design Specification* (PDS) as the final deliverable in this course. (3 credits)

RES9110 Research Topic Rationale

In this course, students articulate the business problem and problem statement which will guide their research project. In addition, they conduct a preliminary literature review to develop the rationale for their research. (3 credits)

Prerequisite: RM9300

RES9120 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. (3 credits)

RES9130 Proposed Research Methodology

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). (3 credits)

RES9140 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)

RES9150 Research Design: Results and Findings

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)

RES9160 Research Design Specification

In this course, students finalize the operational requirements of the proposed research study by producing the *Research Design Specification* (RDS). (3 credits)

Dissertation Development Courses

DST9100 Integration and Implementation Feasibility Testing and Planning

In this course, doctoral candidates implement the approved protocol design by collecting and analyzing data relevant to the feasibility of integrating and implementing the proposed improvement to professional practice.

(2-6 credits)

Prerequisite: RES8130

DST9205 Continuing Dissertation Development

Doctoral candidates requiring additional time to produce an approved dissertation enroll in this course until the dissertation is approved for defense. *(1 credit)*

DST9210 Dissertation Documentation and Defense

In this course, candidates present their findings to the Dissertation Committee at the defense. *(1-6 credit)*

Prerequisite: Approval to Defend

DST9310 Data Collection and Preparation

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)*

Prerequisite: RES9160

DST9320 Data Analysis and Findings

In this course, doctoral candidates implement the approved data analysis plan and review findings with advisors. *(1-6 credits)*

DST9325 Continuing Dissertation Development

Doctoral candidates requiring additional time to produce an approved dissertation enroll in this course until the dissertation is approved for defense. *(1 credit)*

DST9330 Dissertation Documentation and Defense

In this course, doctoral candidates present their findings to the Dissertation Committee at the defense.

(1-3credits)

Prerequisite: Approval to Defend

ELECTIVE COURSES

IA8140 Business Continuity Planning and Recovery

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)*

IA8150 Advanced Topics in Risk and Vulnerability Assessment

In this course, students examine leading tools, technologies and methodologies used in identifying, prioritizing and mitigating information system threats and vulnerabilities; identify and evaluate security controls; and formulate risk mitigation strategies. *(3 credits)*

IA8160 Advanced Topics in Intrusion, Detection and Prevention Methods

In this course, students review case studies describing security incidents and compare, contrast and evaluate the tactical countermeasures taken. *(3 credits)*

IA8170 Advanced Topics in Security Architecture Design Methodologies

In this course, students evaluate the critical factors in selecting and implementing security solutions that support a “defense-in-depth” security architecture. *(3 credits)*

IA8180 Advanced Topics in Wireless Security

This course explores emerging topics such as risks and vulnerabilities, assessment methods and standards associated with wireless technologies. *(3 credits)*

IA8210 Risk Management and Compliance

In this course, students evaluate the procedures and results of risk analysis, as well as the compliance processes that address the regulatory requirements which drive the need for risk analysis within the enterprise. Security-related regulations such as SOX, GLBA, FISMA and HIPAA are examined. *(3 credits)*

PROFESSIONAL DEVELOPMENT COURSES

IC7000 (ISC)² Official CISSP Review Seminar

This course, taught by (ISC)² (an authorized education partner of UoF) provides students with CBK domain review materials and instructor guidance in preparation for the (ISC)² CISSP certification exam. *(0 credits)*