



## *Catalog*

*March 1, 2012 – July 31, 2012*

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

**703.790.3200  
[www.UFairfax.net](http://www.UFairfax.net)**



703.790.3200  
www.UFairfax.net

2070 Chain Bridge Road  
Suite G-100  
Vienna, VA 22182

## GOVERNING DOCUMENTS

The *University of Fairfax Catalog* is the governing document for all academic requirements and program-related information for the University of Fairfax. The *University of Fairfax Student Handbook* specifies rights, responsibilities, and specific policies and procedures as they apply to University of Fairfax students. All University of Fairfax students are bound by the rules, policies and procedures contained in these documents. Official versions of the catalog and the student handbook are posted on the University's website. The catalog and handbook posted most recently to the website supersede previous web and printed versions of these documents and may be downloaded from the University's website and the *Student Information Center* via the *eCollege* learning management platform.

This catalog is valid from March 1, 2012 through July 31, 2012. The University reserves the right to cancel or modify, for any reason, any course or program listed herein. If there is a conflict between the information stated in the catalog and student handbook with that contained in any other document, the information presented in the catalog and student handbook prevails. Policies, regulations, requirements and fees are subject to change without notice at any time at the discretion of the University of Fairfax.

## NOTICE OF NONDISCRIMINATION

The University of Fairfax does not discriminate on the basis of gender, age, race, creed, national origin, sexual orientation or disability in admissions, employment or access to academic programs or student activities.

---

## ACCREDITATION AND CERTIFICATION

The University of Fairfax is accredited by the Accrediting Commission of the Distance Education and Training Council (DETC). The Accrediting Commission of DETC is listed by the U.S. Department of Education as a nationally recognized accrediting agency and is a recognized member of the Council for Higher Education Accreditation (CHEA).



Distance Education and Training Council  
1601 18<sup>th</sup> St. NW, Suite 2  
Washington, DC 20009  
202.234.5100  
<http://www.detc.org>

The University of Fairfax is certified by the State Council of Higher Education for Virginia in accordance with the provisions of Title 23, Chapter 21.1 of the Code of Virginia. The University of Fairfax has been granted the “Certificate to Operate an Institution of Postsecondary Education” authorizing the University of Fairfax to offer degrees, courses for degree credit, or programs of study leading to a degree or certificate in the Commonwealth of Virginia.



State Council of  
Higher Education for Virginia

State Council of Higher Education for Virginia  
101 N. 14TH St., 10TH FL, James Monroe Bldg.  
Richmond, VA 23219  
Tel: (804) 225-2600 Fax: (804) 225-2604  
<http://www.schev.edu>

The University of Fairfax is accredited in Indiana by the ICPPE in accordance with the provisions of Title 21, Chapter 17.1 of the Code of Indiana and applicable regulations of the ICPPE.



The Indiana Commission on Proprietary Education  
302 West Washington Street, Room E201,  
Indianapolis, IN 46204-2767,  
Toll Free Number 1-800-227-5695 or (317) 232-1320  
<http://www.in.gov/cope/directory>

The University of Fairfax, Inc., d/b/a University of Fairfax, is a non-profit (501.c.3) Delaware Corporation.

---

## TABLE OF CONTENTS

<b>GOVERNING DOCUMENTS</b> .....	<b>ii</b>
<b>NOTICE OF NONDISCRIMINATION</b> .....	<b>ii</b>
<b>ACCREDITATION AND CERTIFICATION</b> .....	<b>iii</b>
<b>STATEMENT OF MISSION AND GOALS</b> .....	<b>1</b>
MISSION .....	1
VISION .....	1
INSTITUTIONAL GOALS .....	1
INSTITUTIONAL OBJECTIVES .....	1
MOTTO .....	2
ACCESSIBLE EDUCATION .....	2
<b>ACADEMIC PROGRAMS</b> .....	<b>4</b>
<b>DOCTORATE IN INFORMATION ASSURANCE (DIA)</b> .....	<b>5</b>
Description .....	5
Program Objectives .....	5
Qualifying Exam .....	5
Comprehensive Exams (Level I) .....	6
Credit Requirements .....	6
Earning Graduate Certificates .....	6
<b>DOCTOR OF SCIENCE IN INFORMATION ASSURANCE (DSC)</b> .....	<b>7</b>
Description .....	7
Program Objectives .....	7
Qualifying Exam .....	7
Comprehensive Exams (Level I and II) .....	8
Credit Requirements .....	8
Earning Graduate Certificates .....	8
<b>MASTER OF SCIENCE IN INFORMATION SECURITY MANAGEMENT (MSISM)</b> .....	<b>9</b>
Specializations .....	9
Description .....	9
Program Objectives .....	9
Credit Requirements .....	10
Multiple Specializations .....	10
Earning Graduate Certificates .....	10
<b>MASTER OF SCIENCE IN ENTERPRISE MANAGEMENT (MSEM)</b> .....	<b>11</b>
Specializations .....	11
Description .....	11
Program Objectives .....	11
Credit Requirements .....	11
Earning Graduate Certificates .....	12
<b>GRADUATE CERTIFICATE PROGRAM</b> .....	<b>13</b>
Description .....	13
Program Objectives .....	13
Credit Requirements .....	13
Multiple Graduate Certificates .....	13
Degree Seeking Candidates Earning Graduate Certificates .....	13

<b>ADMISSIONS.....</b>	<b>16</b>
PROGRAM ADMISSION REQUIREMENTS .....	16
DUAL DEGREES .....	16
ADVANCED STANDING .....	16
INTERNATIONAL CREDENTIALS .....	17
ENGLISH LANGUAGE PROFICIENCY .....	17
ADMISSION STATUS .....	17
Formal Admission .....	17
Conditional Admission .....	17
Provisional Admission.....	17
ADMISSION PROCEDURES.....	18
All Programs.....	18
<b>CURRICULA.....</b>	<b>19</b>
Doctorate in Information Assurance (DIA) .....	19
Doctor of Science (DSc) in Information Assurance .....	20
Master of Science in Information Security Management (MSISM).....	21
Master of Science in Enterprise Management (MSEM).....	23
Graduate Certificates .....	24
<b>STUDENT SUPPORT SERVICES.....</b>	<b>27</b>
EXECUTIVE STAFF.....	27
ADMISSIONS .....	27
ACADEMICS.....	27
STUDENT SERVICES.....	28
STUDENT FINANCE.....	28
ADDITIONAL SUPPORT SERVICES .....	29
Orientation.....	29
Student Information Center .....	29
Mobile Access .....	29
Twitter .....	29
Textbooks .....	30
Help Desk .....	30
Electronic Library and Research Resources .....	30
Library Tutorials and Webinars (LIBTUTOR) .....	30
Certification Training Center for Continuing Professional Education .....	31
Additional Doctoral Student Support .....	31
<b>ACADEMIC POLICIES AND PROGRAM EXPECTATIONS.....</b>	<b>32</b>
ACADEMIC CALENDAR.....	32
ACADEMIC TERM .....	32
ACADEMIC YEAR .....	32
ACADEMIC CREDIT POLICY.....	32
ACADEMIC INTEGRITY POLICY.....	32
PROFESSIONAL CONDUCT POLICY.....	33
STUDENT RIGHTS AND RESPONSIBILITIES .....	33
ATTENDANCE.....	33
PARTICIPATION .....	33
TECHNOLOGY REQUIREMENTS .....	34
STANDARDS OF ACADEMIC PROGRESS .....	34
Cumulative Grade Point Average.....	34
Maximum Coursework Allowed .....	34
Completion Rate .....	34
ACADEMIC STANDING .....	34
Good Academic Standing .....	34
Academic Warning .....	35
Academic Probation .....	35
Academic Dismissal .....	35

COMPUTING A CUMULATIVE GRADE POINT AVERAGE (CGPA).....	35
GRADING SCALE .....	36
Incompletes .....	36
Withdrawals.....	36
Audited Courses .....	36
Repeated Courses .....	36
PROGRAM MODIFICATIONS .....	37
Course Substitutions .....	37
Transfer of Course Credits .....	37
Program Modifications for Dual Degree Seekers.....	37
STUDENT IDENTITY VERIFICATION.....	37
PROCTORED EXAMS .....	38
Master’s Degrees .....	38
Doctoral Degrees .....	38
CONTINUOUS ENROLLMENT/GOVERNING RULES .....	38
TIME LIMIT FOR COMPLETION.....	38
GRADUATION REQUIREMENTS .....	39
All Graduates.....	39
Graduates of the Doctoral Program .....	39
Alternate Degree Award for Doctoral Students.....	39
TRANSCRIPT REQUESTS.....	39
<b>FINANCIAL INFORMATION.....</b>	<b>40</b>
TUITION.....	40
FEES .....	40
SPECIAL SERVICES FEES.....	40
Advanced Standing Evaluation .....	40
Dissertation Quality Review .....	40
Registration .....	41
Review Seminar Fee.....	41
Student Services .....	41
Technology .....	41
Transfer Credit.....	41
FINANCIAL POLICIES .....	41
Add/Drop Period .....	41
Withdrawals.....	41
Refunds.....	42
FINANCIAL ASSISTANCE.....	42
Program and Lifetime Maximums .....	42
FORMS OF FINANCIAL ASSISTANCE.....	42
Military Spouse Career Advancement Accounts (MyCAA) .....	42
Employer Tuition Reimbursement/ Direct Billing .....	43
Scholarships, Fellowships and Loans .....	43
<b>COURSE DESCRIPTIONS.....</b>	<b>45</b>
CORE COURSES .....	45
SPECIALIZATION COURSES .....	47
ELECTIVE COURSES.....	48
RESEARCH COURSES .....	49
PROFESSIONAL DEVELOPMENT COURSES.....	53
<b>FACULTY.....</b>	<b>54</b>
<b>PROFESSIONAL ADVISORY COUNCIL .....</b>	<b>63</b>
<b>BOARD OF DIRECTORS .....</b>	<b>72</b>
<b>ACADEMIC CALENDAR .....</b>	<b>73</b>

## **STATEMENT OF MISSION AND GOALS**

### **MISSION**

The mission of the University of Fairfax is to support the cybersecurity community by providing adult learners with quality, accessible, distance education. The practitioner-oriented graduate programs offered produce applied research in Enterprise Management, focusing on Information Assurance and Information Security.

### **VISION**

The University supports this mission by developing curricula which are continually improved through outcomes assessment and consultation with practitioner faculty. UoF delivers its programs through an accessible, interactive, collaborative online educational environment which strengthens learning and facilitates critical thinking, problem-solving, and applied research competencies. Finally, it supports students with services that foster academic success.

### **INSTITUTIONAL GOALS**

- To help address a critical global priority
- To operate with integrity
- To support the cybersecurity community
- To meet the career path needs of adult professionals
- To maintain currency with cybersecurity trends and technology
- To sustain a learner-centered institutional culture
- To foster processes of continual improvement
- To be recognized as a thought leader
- To preserve an institutional commitment to providing quality distance education

### **INSTITUTIONAL OBJECTIVES**

The objectives of the University of Fairfax ensure that its practitioner-oriented curricula are continually improved through outcomes assessment and consultation with stakeholders; that students apply critical thinking skills and applied research competencies to cybersecurity challenges; that graduates apply theory, concepts and skills which contribute to their career advancement; that learners utilize a multi-disciplinary approach for problem solving in order to address the needs of the enterprise; and that the University generates the resources to maintain the University's programs.

## MOTTO

The rationale for the founding of the University is encapsulated in the University motto: *Secure Your Future* or *Munite Futurum* in Latin, as displayed on the University's seal. In essence, the motto expresses that earning a University of Fairfax degree enables students and alumni to contribute to "securing the future" of the nation, while also helping to secure their own, as they become cybersecurity leaders in a field for which there is a continuing and ever-increasing demand.

## ACCESSIBLE EDUCATION

The goals and objectives of the University of Fairfax are attained through the accessible, online delivery of its programs. Courses are delivered via the *Pearson eCollege Learning Studio* (more familiarly known as *eCollege*), utilizing both synchronous and asynchronous instruction. Project-driven courses may be accessed online from any location, at times which fit the busy schedules of adult students, thus providing working professionals the flexibility and convenience they need to easily communicate with faculty members and fellow students. Students progress through their programs in groups or cohorts. The cohort model is designed to meet the unique needs of adult learners. Smaller groups provide opportunities for collaborative learning and support, as well as more personalized instruction and advising.

## **HISTORICAL PERSPECTIVE**

The University of Fairfax (UoF) was accredited by the Accrediting Commission of the Distance Education and Training Council (DETC) on January 20, 2012. The Accrediting Commission of DETC is listed by the U.S. Department of Education as a nationally recognized accrediting agency and is a recognized member of the Council for Higher Education Accreditation (CHEA). DETC is the leader in accrediting global distance learning with more than 4 million students enrolled in DETC accredited institutions. ([www.detc.org](http://www.detc.org)).

The University's attainment of accreditation caps a 10 year history of student and alumni accomplishments in the cybersecurity sector. Successful University of Fairfax students and graduates serve as cybersecurity specialists, executives and policy-makers in the public and private sectors. Major employers including SAIC, Northrop Grumman, CSC, Lockheed Martin, Wells Fargo, Dell, NSA, DHS, Dept. of Treasury and Veterans Affairs hire and promote our students and alumni.

In order to reach the historic milestone of accreditation UoF conducted a comprehensive and rigorous process of self-evaluation; submitted its online doctoral degrees, master's degrees and graduate certificate program materials for review by subject matter specialists; and hosted onsite review teams of evaluators. As part of the evaluation process, DETC conducted surveys of students and alumni which consistently resulted in over 95 % satisfaction.

The University of Fairfax was established in 2002 in response to the events of 9/11 and in support of the federal efforts to increase the nation's cybersecurity by providing high quality, online doctoral, master's and graduate certificate programs for adult learners. In contrast to other graduate institutions which offer information security/assurance only as a concentration as part of a degree program, UoF has dedicated the entire institution to degree and certificate programs in pursuit of excellence in cybersecurity.

This exclusive focus on cybersecurity distinguishes the University and provides professionals seeking to advance in the field, as well as their employers and clients, an innovative approach for addressing growing professional demand in a rapidly evolving area. Our students and alumni have benefited from this comprehensive cybersecurity focus and from our expert practitioner faculty, both of which have enabled them to be hired and promoted at senior levels by major employers.

The State Council of Higher Education for Virginia (SCHEV) certified UoF as an institution of higher learning in 2002. Over the next year, a select group of educators and senior cybersecurity practitioners from organizations including Ernst & Young, Anteon, CSC and the Defense Information Systems Agency (DISA), developed a curriculum designed to meet the needs of cybersecurity employers. This group of professionals became the initial faculty of the University.

In July 2003, the University enrolled its first cohort of graduate students in its unique cybersecurity graduate degree programs. The first graduates of UoF earned their Master of Science degrees in October 2004; the University awarded its first doctoral degrees in February 2007. Since 2004, online delivery of our programs has made the University's programs accessible to professionals worldwide and has even enabled faculty members and students on active duty to participate.

## ACADEMIC PROGRAMS

The University of Fairfax is approved to offer the following graduate programs:

- **Doctorate in Information Assurance**
- **Doctor of Science in Information Assurance**
- **Master of Science in Information Security Management** with specializations in:
  - Information Security Analysis (ISA)
  - Information Security Auditing (IAU)
  - Information System Certification (ISC)
  - Information Security Engineering (ISE)
  - Information Security Research (ISR)
- **Master of Science in Enterprise Management** with specializations in:
  - Information Security Analysis (ISA)
- **Graduate Certificates** in:
  - Cybersecurity Best Practices (CBP)
  - Information Security Professional Practices (ISPP)
  - Information Security Analysis (ISA)
  - Information Security Auditing (IAU)
  - Information System Certification (ISC)
  - Information Security Engineering (ISE)
  - Information Security for the Enterprise (ISEN)
  - Certified Cybersecurity Researcher (CCR)
  - Information Security Research Practices (ISRP)
  - Knowledge-Based Research for Information Security Practitioners (KRIS)
  - Solution-Based Research for Information Security Practitioners (SRIS)

---

## **DOCTORATE IN INFORMATION ASSURANCE (DIA)**

### **Description**

This degree program helps students to advance their careers as consultants or professional managers in the Information Security and Assurance field. In this program, students undertake solution-oriented applied field research projects which address relevant industry problems and contribute to the advancement of knowledge in the practice of Information Assurance.

This program fosters the development of students who:

- Are recognized as practitioners with expertise in a specialized field of study relevant to the cybersecurity community
- Apply critical thinking and problem-solving skills in the analysis of information assurance issues
- Utilize an evidence-based approach to solution identification when addressing problems relevant to the cybersecurity community
- Demonstrate competence in conducting solution-focused field research relevant to information assurance practitioners
- Make continuing contributions to knowledge and practice in the field of cybersecurity

### **Program Objectives**

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
- Demonstrate secondary research competencies in the investigation and identification of problems experienced by information assurance practitioners
- Develop evidence-based recommendations for solutions which address problems relevant to the cybersecurity community
- Empirically assess the feasibility of a proposed solution for a problem affecting the cybersecurity community
- Articulate a thorough understanding of a specialized field of study relevant to the cybersecurity community

### **Qualifying Exam**

Doctoral students enrolled in the DIA 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)**

Doctoral students enrolled in the DIA 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. 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 60 semester credits beyond a Master's degree, including 57 credits of pre-dissertation courses (consisting of 24 credits of Information Security content taken from core and specialization courses, 18 credits of research methods courses, 6 credits of comprehensive exam courses, 9 credits of research-preparation courses) and 3 credits of dissertation development courses.

To ensure that doctoral students make steady progress towards the completion of their dissertations, the University has developed the *Dissertation Project Plan*. This plan consists of a series of deliverables students produce in research methods courses and dissertation courses.

In the preliminary Research Methods courses (*RM6000, RM8250, RM8500, RM9100*), DIA students are introduced to the research paradigm and develop research skills through the completion of course deliverables. In later Research Methods courses (*RM9150, RM9200*) students follow a structured approach for selecting a research site and identifying a research topic.

In the Research Preparation courses (*RES8110-RES8140*) doctoral students develop the *Feasibility Study Specification (FSS)* which describes the proposed research study. Candidacy is granted after approval of the FSS.

Once doctoral candidates in the DIA program complete the research preparation courses, they enroll in Dissertation Development courses (*DST8110-DST8130*) during which they conduct the approved research and complete the dissertation.

Finally, prior to conferral of the degree, the doctoral candidate must successfully defend the doctoral dissertation in an oral presentation before the Dissertation Committee.

## **Earning Graduate Certificates**

DIA students 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 under the *Graduate Certificate Program* section in this document.

---

## DOCTOR OF SCIENCE IN INFORMATION ASSURANCE (DSc)

### 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

### 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 (consisting of 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.

To ensure that doctoral students make steady progress towards the completion of their dissertations, the University has developed the *Dissertation Project Plan*. This plan consists of a series of deliverables students produce in research methods courses and dissertation courses.

In the preliminary Research Methods courses (*RM6000, RM8250, RM8500, RM9100*), DSc students are introduced to the research paradigm and develop research skills through the completion of course deliverables. In later Research Methods courses (*RM9150, RM9250*) students follow a structured approach for selecting a research site and identifying a research topic.

In the Research Preparation courses (*RES8510-RES8580*) doctoral students proceed under the guidance of an advisor and develop the required proposals. Candidacy is granted after approval of the *Proposed Research Plan (PRP)*. DSc students are granted permission to conduct research after approval of the *Research Design Specification (RDS)*.

Once doctoral candidates in the DSc program complete the research preparation courses, they enroll in Dissertation Development courses (*DST8510-DST8540*) during which they conduct the approved research and complete the dissertation.

Finally, prior to conferral of the degree, the doctoral candidate must successfully defend the doctoral dissertation in an oral presentation before the Dissertation Committee.

## Earning Graduate Certificates

DSc students 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 under the *Graduate Certificate Program* section in this document.

---

## MASTER OF SCIENCE IN INFORMATION SECURITY MANAGEMENT (MSISM)

### Specializations

- Information Security Analysis (ISA)
- Information Security Auditing (IAU)
- Information System Certification (ISC)
- Information Security Engineering (ISE)
- Information Security Research (ISR)

### Description

This degree program prepares students to be strategic and tactical contributors in the development, implementation and evaluation of enterprise level security programs. Specializations allow students to pursue a program of study which relates to their professional interests and goals.

This program fosters the development of students who:

- Are recognized as knowledgeable and qualified practitioners in a specialized field of information security
- Possess a depth of knowledge in current cybersecurity practices
- Apply critical thinking and problem-solving skills in the analysis of issues relevant to the cybersecurity community
- Utilize secondary research competencies in the investigation and selection of best practice solutions to information security challenges
- Demonstrate the knowledge and skills necessary to address a specialized area of information security management

### Program Objectives

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

- Compile, analyze, and assess the applicability of best practices in addressing information security issues relevant to the cybersecurity community
- Evaluate the impact of business constraints and processes on the implementation of information security programs
- Integrate principles and techniques of risk analysis, project planning and change management in the development of information security strategies
- Demonstrate secondary research skills in the investigation and selection of best practice solutions to address information security challenges
- Demonstrate mastery of theory, concepts and skills in addressing specialized aspects of information security management

---

## **Credit Requirements**

The MSISM degree program consists of 36 semester credits beyond a baccalaureate degree, including 18 credits of core courses, 6 credits of research methods courses, and 12 credits of specialization-specific courses.

## **Multiple Specializations**

MSISM degree students may pursue multiple specializations through the completion of graduate certificates. Each specialization requires completion of four specialization-specific courses. Required specialization courses may apply to multiple certificates.

## **Earning Graduate Certificates**

MSISM students complete the requirements for a 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 under the *Graduate Certificate Program* section in this document.

## **Specialization Options**

The University of Fairfax offers a variety of specialization options to meet the needs of information security professionals.

### ***Information Security Analysis (ISA)***

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

### ***Information Security Auditing (IAU)***

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

### ***Information System Certification (ISC)***

Students develop competencies in supporting a management structure to certify and accredit information systems by developing policies, standards and procedures in accordance with a prescribed set of criteria.

### ***Information Security Engineering (ISE)***

Students develop competencies in assessing network vulnerabilities and attack methods as well as in designing and deploying counter-measures and resilient security architectures.

### ***Information Security Research (ISR)***

Doctoral students who have completed a minimum of 36 semester credits of a University of Fairfax doctoral degree program, but wish to discontinue studies, may be awarded an MSISM degree in *Information Security Research*.

## **MASTER OF SCIENCE IN ENTERPRISE MANAGEMENT (MSEM)**

### **Specializations**

- Information Security Analysis (ISA)

### **Description**

This degree program prepares students to be strategic and tactical contributors in the development, implementation and evaluation of enterprise level programs. Specializations allow students to pursue a program of study which relates to their professional interests and goals.

This program fosters the development of students who:

- Are recognized as knowledgeable and qualified practitioners in a specialized field of enterprise management
- Apply critical thinking and problem-solving skills in the analysis of issues relevant to enterprise managers
- Utilize secondary research competencies in the investigation and selection of best practice solutions to enterprise challenges
- Demonstrate the knowledge and skills necessary to address a specialized area of enterprise management

### **Program Objectives**

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

- Compile, analyze, and assess the applicability of best practices in addressing enterprise management issues
- Evaluate the impact of business constraints and processes on the implementation of enterprise programs
- Integrate principles and techniques of risk analysis, project planning and change management in the development of enterprise strategies
- Demonstrate secondary research skills in the investigation and selection of best practice solutions to address enterprise challenges
- Demonstrate mastery of theory, concepts and skills in addressing specialized aspects of enterprise management

### **Credit Requirements**

The MSEM degree program consists of 36 semester credits beyond a baccalaureate degree, including 18 credits of core courses, 6 credits of research methods courses, and 12 credits of specialization-specific courses.

### **Earning Graduate Certificates**

MSEM students 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 under the *Graduate Certificate Program* section in this document.

### **Specialization Options**

The University of Fairfax offers a variety of specialization options to meet the needs of enterprise management professionals.

#### ***Information Security Analysis (ISA)***

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

## **GRADUATE CERTIFICATE PROGRAM**

### **Description**

Graduate certificates represent a level of achievement of technical competencies and project experience which relate to specialized fields of practice in Information Security.

Requirements for earning a graduate certificate cannot be satisfied through transfer credit.

Upon acceptance into a University of Fairfax degree program, students who have earned a grade of “B” or better in graduate certificate courses may request that those credits be applied to meet degree requirements.

This program fosters the development of students who:

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

### **Program Objectives**

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

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

### **Credit Requirements**

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

### **Multiple Graduate Certificates**

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

### **Degree Seeking Candidates Earning Graduate Certificates**

Degree 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).

## **Graduate Certificate Options**

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

### ***Cybersecurity Best Practices (CBP)***

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

### ***Information Security Professional Practices (ISPP)***

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

### ***Information Security Analysis (ISA)***

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

### ***Information Security Auditing (IAU)***

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

### ***Information System Certification (ISC)***

Students develop competencies in supporting a management structure to certify and accredit information systems by developing policies, standards and procedures in accordance with a prescribed set of criteria.

### ***Information Security Engineering (ISE)***

Students develop competencies in assessing network vulnerabilities and attack methods as well as in designing and deploying counter-measures and resilient security architectures.

### ***Information Security for the Enterprise (ISEN)***

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

In addition, students enrolled in doctoral degree programs may earn the following graduate certificates as they progress through their programs.

***Certified Cybersecurity Researcher (CCR)***

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

***Information Security Research Practices (ISRP)***

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

***Knowledge-Based Research for Information Security Practitioners (KRIS)***

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

***Solution-Based Research for Information Security Practitioners (SRIS)***

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

## ADMISSIONS

### PROGRAM ADMISSION REQUIREMENTS

Applicants are evaluated individually based on their professional experience, academic credentials from accredited institutions and admissions interview, to assess their potential for completing the relevant academic program successfully. The table below summarizes the minimum requirements for admission to each program offered by the University.

Program Name	Relevant Professional Experience	Required Degrees from Accredited Institution(s)
DIA	Min. 5 Years	Master's
DSc	Min. 5 Years	Master's
DSc with Advanced Standing	Min. 8 Years	Two Master's, or a Professional Degree (e.g., JD), or "ABD" Status*
MSISM	Min. 3 Years	Baccalaureate
MSEM	Min. 3 Years	Baccalaureate
MSISM/DIA or MSISM/DSc (Dual Degree)	Min. 3 Years	Baccalaureate
Graduate Certificate	Min. 3 Years	90 Semester Credits

\* completed all required pre-dissertation coursework of a doctoral program

### DUAL DEGREES

Students may apply for a program of study which leads to two consecutive degrees (MSISM/DIA or MSISM/DSc) on an accelerated schedule. These students are required to follow a program of study which includes core, specialization-specific, elective, research and dissertation courses. The MSISM degree is awarded upon successful completion of the required 36 semester credits. Formal admission to the doctoral program selected is granted upon successful completion of the MSISM degree.

### ADVANCED STANDING

Applicants with at least eight years of relevant experience who hold one of the following from an accredited institution: a professional degree (e.g., Juris Doctorate); more than one master's degree; or have completed all required pre-dissertation coursework in a doctoral program (i.e., have achieved "ABD" status) within the past 10 years may apply for advanced standing in the Doctor of Science (DSc) program. Such students are required to complete a program of study which consists of a minimum of 60 semester credits, including courses in research methods, research design and dissertation development.

## **INTERNATIONAL CREDENTIALS**

Applicants with international credentials must arrange for a course-by-course evaluation of their transcripts to confirm equivalence to an accredited degree from the U.S. The University of Fairfax accepts evaluations provided by World Education Services (WES), American Association of Collegiate Registrars and Admissions Officers (AACRAO), Educational Credential Evaluators (ECE) or International Educational Research Foundation (IERF). If the academic records are in a language other than English, an English translation is required that is as close to word-for-word as possible.

## **ENGLISH LANGUAGE PROFICIENCY**

Applicants for any degree program whose native language is not English and who have not earned a degree from an appropriately accredited institution where English is the principal language of instruction must receive a minimum score of 550 on the paper-based Test of English as a Foreign Language (TOEFL), or its equivalent.

## **ADMISSION STATUS**

### **Formal Admission**

Applicants who meet the admissions requirements of the University and submit official transcripts are granted formal admission.

### **Conditional Admission**

Applicants who meet the admissions requirements of the University and submit unofficial transcripts are granted conditional admission. In all cases, official transcripts must be received prior to the start of the student's second registration period in order to remain enrolled.

### **Provisional Admission**

Applicants who do not meet the admissions requirements of the University may submit a petition for consideration of an exception. If the petition is approved, the student is granted provisional admission and must comply with additional requirements, as determined on an individual basis, depending on the exception granted. For these applicants, formal admission will be granted upon successful completion of the requirements specified in the letter approving the student's petition.

Students applying for dual degrees (MSISM/DIA or MSISM/DSc) may be granted provisional admission to the selected doctoral program without the need for a petition, provided conditional or formal admission to the MSISM degree has been granted.

## **ADMISSION PROCEDURES**

### **All Programs**

To be admitted to a degree or certificate program, applicants must:

- complete and submit the Application for Admission along with a \$75 application fee.
- complete and submit the Application for Doctoral Program if applicable.
- submit proof of graduation or previous credits earned. (Acceptable documents include an Issued to Student transcript or copy of a diploma.)
- submit a resume or summary of employment history.
- complete a telephone interview with an Admissions Officer.
- request an official academic transcript from the institution which awarded the applicant's highest degree earned, to be received by the University no later than the end of the student's first academic term.
- submit TOEFL scores, if applicable.

Information provided in these application materials is used by the University in making admissions decisions and may be verified through official transcripts, reference checks, and/or credit reports.

## CURRICULA

### Doctorate in Information Assurance (DIA)

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

**Core Courses:**

IA7020	<i>Information Security Systems and Organizational 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>

**Specialization Courses:**

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>

**Comprehensive Exam Courses:(two of the following)**

CEX8220	<i>Security Program Strategies and Implementation (Level I)</i>
CEX8230	<i>Legal and Ethical Management Issues in Information Security (Level I)</i>
CEX8240	<i>Strategic and Technological Trends in Information Security (Level I)</i>

**Research Methods Courses:**

RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>
RM8500	<i>Research Foundations for Information Security Practitioners</i>
RM9100 <sup>1</sup>	<i>Qualitative and Quantitative Analysis</i>
RM9150	<i>Feasible Problem-Driven Research in Information Security</i>
RM9200	<i>Designing Solutions to Information Security Problems</i>

**Research Preparation Courses:**

RES8110	<i>Research Needs and Requirements Analysis</i>
RES8120	<i>Identification of Evidence-Based Solutions</i>
RES8130	<i>Operational Design and Specification</i>
RES8140 <sup>2</sup>	<i>Continuing FSS Development</i>

**Dissertation Development Courses:**

DST811X <sup>3</sup>	<i>Feasibility Testing and Planning</i>
DST8120 <sup>3</sup>	<i>Continuing Dissertation Development</i>
DST813X <sup>4</sup>	<i>Dissertation Documentation and Defense</i>

**Minimum credits required for DIA: 60<sup>4</sup>**

<sup>1</sup> Comprehensive Exams must be completed and passed prior to enrollment in this course.

<sup>2</sup> This course must be repeated until deliverables are approved.

<sup>3</sup> Course number varies based on number of credit hours earned.

<sup>4</sup> Credit hours may exceed the minimum stated if dissertation deliverables are not completed within expected timeframes.

---

**Doctor of Science (DSc) in Information Assurance**

**Course #      Course Title**

---

**Core Courses:**

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

**Specialization Courses:**

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>

**Comprehensive Exam Courses:**

**Two of the following:**

CEX8220	<i>Security Program Strategies and Implementation (Level I)</i>
CEX8230	<i>Legal and Ethical Management Issues in Information Security (Level I)</i>
CEX8240	<i>Strategic and Technological Trends in Information Security (Level I)</i>

**Plus:**

CEX9200	<i>Research Topics in Information Security (Level II)</i>
---------	---

**Research Methods Courses:**

RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>
RM8500	<i>Research Foundations for Information Security Practitioners</i>
RM9100 <sup>5</sup>	<i>Qualitative and Quantitative Analysis</i>
RM9150	<i>Feasible Problem-Driven Research in Information Security</i>
RM9250	<i>Building a Knowledge-Base in the Information Security Discipline</i>

**Research Preparation Courses:**

RES8510	<i>Research Topic Rationale</i>
RES8520	<i>Review and Synthesis of Prior Research</i>
RES8530	<i>Proposed Research Methodology</i>
RES8540 <sup>6</sup>	<i>Continuing PRP Development</i>
RES8550	<i>Research Design: Data Collection Plan</i>
RES8560	<i>Research Design: Results and Findings</i>
RES8570	<i>Research Design Specification</i>
RES8580 <sup>7</sup>	<i>Continuing RDS Development</i>

**Dissertation Development Courses:**

DST851X <sup>7</sup>	<i>Data Collection and Preparation</i>
DST852X <sup>8</sup>	<i>Data Analysis and Findings</i>
DST8530 <sup>7</sup>	<i>Continuing Dissertation Development</i>
DST854X <sup>8</sup>	<i>Dissertation Documentation and Defense</i>

**Minimum credits required for DSc: 70<sup>8</sup>**

---

<sup>5</sup> Comprehensive Exams must be completed and passed prior to enrollment in this course.

<sup>6</sup> This course must be repeated until deliverables are approved.

<sup>7</sup> Course number varies based on number of credit hours earned.

<sup>8</sup> Credit hours may exceed the minimum stated if dissertation deliverables are not completed within expected timeframes.

---

**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 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:***

IA8125	<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 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:***

IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8110	<i>Certification and Accreditation</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>
IA8210	<i>Risk Management and Compliance</i>

***Credits required for MSISM: 36***

---

***Specialization: Information System Certification (ISC)***

***Course #      Course Title***

---

***Core Courses:***

IA7020	<i>Information Security Systems and Organizational 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:***

IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8110	<i>Certification and Accreditation</i>
IA8140	<i>Business Continuity Planning and Recovery</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>

***Credits required for MSISM: 36***

***Specialization: Information Security Engineering (ISE)***

***Course #      Course Title***

---

***Core Courses:***

IA7020	<i>Information Security Systems and Organizational 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>
EM8010	<i>Business Risk Analysis</i>
PM8000	<i>Project Management</i>
EM9200	<i>Strategic Analysis</i>

***Research Methods Courses:***

RM6100	<i>Effective Writing</i>
RM8200	<i>Web-Based Research Methods</i>

***Specialization Courses:***

IA8125	<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**

***Cybersecurity Best Practices-CISSP (CBP)***

***Course # Course Title***

---

IA7020	<i>Information Security Systems and Organizational Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IC7000 <sup>9</sup>	<i>(ISC)<sup>2</sup> Official CISSP Review Seminar</i>

***Credits required for Certificate: 6***

***Information Security Professional Practices (ISPP)<sup>10</sup>***

---

IA7020	<i>Information Security Systems and Organizational 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***

***Information Security Analysis (ISA)***

---

IA8125	<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 Certificate: 12***

***Information Security Auditing (IAU)***

---

IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8110	<i>Certification and Accreditation</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>
IA8210	<i>Risk Management and Compliance</i>

***Credits required for Certificate: 12***

---

<sup>9</sup> Students must provide verification of attendance at an (ISC)<sup>2</sup> Official CISSP Review Seminar.

<sup>10</sup> Upon completion of this certificate the student is awarded the NSA 4011 Certification for Information Systems Security Professionals (CNSS No.4011) and the NSA 4012 Certification for Senior Systems Managers (CNSS No. 4012).

---

**Information System Certification (ISC)**

**Course # Course Title**

---

IA8030	<i>Design, Development and Evaluation of Security Controls</i>
IA8110	<i>Certification and Accreditation</i>
IA8140	<i>Business Continuity Planning and Recovery</i>
IA8190	<i>Forensic Evaluation and Incident Response Management</i>

**Credits required for Certificate: 12**

**Information Security Engineering (ISE)**

---

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 Certificate: 12**

**Information Security for the Enterprise (ISEN)**

---

IA7020	<i>Information Security Systems and Organizational Awareness</i>
IA7030	<i>Legal and Ethical Practices in Information Security</i>
IA7040	<i>Information Security and Organizational Change</i>
PM8100	<i>Information Security Project Management</i>

**Credits required for Certificate: 12**

**Certified Cybersecurity Researcher (CCR)<sup>11</sup>**

---

RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>
RM8500	<i>Research Foundations for Information Security Practitioners</i>

**At least two of the following:**

CEX8220	<i>Security Program Strategies and Implementation (Level I)</i>
CEX8230	<i>Legal and Ethical Management Issues in Information Security (Level I)</i>
CEX8240	<i>Strategic and Technological Trends in Information Security (Level I)</i>
CEX9200	<i>Research Topics in Information Security (Level II)</i>

**Credits required for Certificate: 15**

**Information Security Research Practices (ISRP)<sup>12</sup>**

---

RM6000	<i>Effective Writing in Information Security Analysis</i>
RM8250	<i>Web-Based Research Methods in Information Security</i>
RM8500	<i>Research Foundations for Information Security Practitioners</i>
RM9100	<i>Qualitative and Quantitative Analysis</i>
RM9150	<i>Feasible Problem-Driven Research in Information Security</i>

**At least one of the following:**

RM9200	<i>Designing Solutions to Information Security Problems</i>
RM9250	<i>Building a Knowledge-Base in the Information Security Discipline</i>

**Credits required for Certificate: 18**

---

<sup>11</sup> Student must be enrolled in a doctoral program to earn this certificate.

<sup>12</sup> Student must be enrolled in a doctoral program to earn this certificate.

---

***Knowledge-Based Research for Information Security Practitioners (KRIS)<sup>13</sup>***

***Course # Course Title***

---

RES8510	<i>Research Topic Rationale</i>
RES8520	<i>Review and Synthesis of Prior Research</i>
RES8530	<i>Proposed Research Methodology</i>
RES8550	<i>Research Design: Data Collection Plan</i>
RES8560	<i>Research Design: Results and Findings</i>
RES8570	<i>Research Design Specification</i>

***Credits required for Certificate: 18***

***Solution-Based Research for Information Security Practitioners (SRIS)<sup>14</sup>***

---

RES8110	<i>Research Needs and Requirements Analysis</i>
RES8120	<i>Identification of Evidence-Based Solutions</i>
RES8130	<i>Operational Design and Specification</i>

***Credits required for Certificate: 9***

---

<sup>13</sup> Student must be enrolled in the Doctor of Science (DSc) program to earn this certificate.

<sup>14</sup> Student must be enrolled in the Doctorate of Information Assurance (DIA) program to earn this certificate.

## **STUDENT SUPPORT SERVICES**

### **EXECUTIVE STAFF**

#### ***President***

The President implements policy and directs all functions of the University.

### **ADMISSIONS**

#### ***Admissions Officer***

The Admissions Officer serves as the student's first contact and advisor during the admissions process.

#### ***Vice President of Admissions and Marketing***

The Vice President of Admissions and Marketing is available as an additional resource to students during the admissions process and throughout their matriculation at the University of Fairfax.

### **ACADEMICS**

#### ***Chief Academic Officer***

The Chief Academic Officer (CAO) oversees academic affairs and directs all UoF graduate education programs. The CAO has responsibility for the administration of academic programs including faculty appointment and development, curriculum development and review, and management of the delivery of these programs. The Chief Academic Officer (CAO) is the final recourse for academic decisions.

#### ***Dean of Academic Systems, Services and Assessment***

The Dean of Academic Systems, Services and Assessment (DASSA) oversees the delivery of courses and serves as the primary academic advisor to students prior to research related courses.

#### ***Dean of Doctoral Research***

The Dean of Doctoral Research (DDR) is the final authority with respect to the dissertation approval process, ensuring that the dissertation deliverables meet the quality standards of the University. The DDR serves as the subject matter expert for research-related courses and oversees the Director of Doctoral Advising and Dissertation Advisors.

#### ***Director of Doctoral Advising***

The Director of Doctoral Advising (DDA) assists the DDR in evaluating training and development needs of Dissertation Advisors and serves as an academic resource to doctoral students during their dissertation coursework.

#### ***Director of Curriculum Content – Information Security***

The Director of Curriculum Content – Information Security (DCC-IS) serves as the subject matter expert for Information Security courses. The DCC-IS evaluates and assesses the overall integration of course objectives with the degree requirements and goals, ensuring the academic rigor and quality of the degree programs offered by the University.

### ***Director of Curriculum Content – Enterprise Management***

The Director of Curriculum Content – Enterprise Management (DCC-EM) serves as the subject matter expert for Enterprise Management courses. The DCC-EM evaluates and assesses the overall integration of course objectives with the degree requirements and goals, ensuring the academic rigor and quality of the degree programs offered by the University.

### ***Dissertation Advisors***

Dissertation advisors serve as the primary mentors for doctoral students as they progress through the Dissertation Project Plan and support them as they develop the dissertation deliverables.

### ***Faculty Advisors***

Faculty members are the content experts for their courses and share their practical experience and knowledge with students through frequent interaction via online threaded discussions, email, conference calls and chat rooms. During the term faculty members are available for individual counseling and advice. Faculty members also serve as mentors to students by providing career-related guidance throughout their programs.

## **STUDENT SERVICES**

### ***Academic Operations Coordinator***

The Academic Operations Coordinator (AOC) supports multiple facets of the University's online environment and academic operations to meet the needs of both students and faculty.

### ***Academic Services Coordinator***

The Academic Services Coordinator (ASC) supports multiple facets of the University's student services to meet the needs of new, continuing and returning students.

### ***Academic Records Coordinator / Assistant Registrar***

The Academic Records Coordinator (ARC) /Assistant Registrar (AR) maintains the student academic records, confirms student registration, and provides support to the Registrar.

### ***Online Librarians***

The Online Librarians provide reference assistance to students and conduct online tutorials to support students in developing secondary research skills.

### ***Registrar***

The Registrar provides oversight for the maintenance of student academic records and confirms the evaluation of transfer credits.

## **STUDENT FINANCE**

### ***Controller***

The Controller provides oversight for the maintenance of student financial records and supervises student financial services

### ***Financial Services Coordinator***

The Financial Services Coordinator (FSC) maintains student financial records and is the point of contact for student finance questions.

---

## ADDITIONAL SUPPORT SERVICES

### Orientation

To ensure a productive and beneficial educational experience at the University of Fairfax, students participate in an online orientation. Before students begin their first courses, they are given access to the *Orientation Center* and the *Student Information Center* on the *eCollege* platform. The *Orientation Center* includes information on:

- the *eCollege* platform and features commonly used in online courses,
- the academic integrity policy, and
- resources for students such as the catalog, student handbook and curriculum overviews.

In addition, students attend an online Orientation session which covers:

- expectations, guidelines, and requirements for students,
- policies, procedures and forms, and
- information on student support services and resources.

In preparation for this session, students complete a number of steps which are listed in the *New Student Checklist*, including the submission of an electronic copy of a government-issued photo identification which is used for student identity verification.

### Student Information Center

The *Student Information Center* (SIC) is an online gateway to information for students. Available within *eCollege*, the SIC is presented within a familiar course structure as *UOF101*. Through the SIC, students can:

- Download catalog, handbooks and forms;
- View the academic calendar;
- Review upcoming schedules and syllabi; and
- Access faculty, students and staff through e-mail.

### Mobile Access

Students who use smart phone technology may access certain portions of their courses such as discussion threads and *Gradebook* by using the University's *mSite*. This mobile-accessible website (<http://m.ufairfaxonline.net>) supports browser enabled phones such as Androids, iPhones and WindowsPhones.

### Twitter

Students may subscribe to Twitter feeds from UoF Academics to ensure they get timely notice of important deadlines and announcements. Students may sign up to follow the University by visiting <http://www.twitter.com> and following @UoFAcademics.

---

## Textbooks

The Master Booklist which identifies required and optional textbooks for all courses is posted in the *Student Information Center* (SIC) in *eCollege* and on the University's website. Direct links to *Amazon* and *CourseSmart* (eBooks) for purchasing books are also available in the SIC.

## Help Desk

For technical assistance, *eCollege* provides a 24-hour Help Desk which is available seven days a week at 877.740.2213.

## Electronic Library and Research Resources

The University of Fairfax maintains a virtual library that provides access to a variety of resources. Through an online internet portal within the *eCollege* platform, these resources are available to students and faculty for conducting secondary research 24 hours a day, seven days a week. This portal provides access to:

- ACM Digital Library
- Directory of Open Access Journals
- Education Resources Information Center (ERIC)
- Government Enterprise Vendor Research Library
- IBM Corporation Research & Development Journals
- IEEE Publications
- ISACA Information Systems Control Journal
- Library and Information Resources Network (LIRN)
- National Institute of Standards and Technology (NIST) Virtual Library
- National Technical Information Service (NTIS)
- Networked Digital Library of Theses and Dissertations (NDLTD)

## Library Tutorials and Webinars (LIBTUTOR)

The Online Librarians conduct tutorials using *ClassLive Pro* within the *eCollege* platform in the LIBTUTOR course shell. The following is a list of tutorials which are held on a regularly scheduled basis:

- Orientation to the Library Portal
- Boolean Search Techniques
- Orientation to TurnItIn.com
- Searching IEEE Periodicals
- Searching ACM Databases
- Using Resources in LIRN

### **Certification Training Center for Continuing Professional Education**

The *Certification Training Center for Continuing Professional Education* was established to support the continuing professional education needs of students and alumni. Through this center, the University provides support by co-sponsoring information security certification training and provides complimentary online tools to aid in preparing for the CISSP certification exam.

### **Additional Doctoral Student Support**

#### ***Dissertation Bootcamp***

Doctoral students present their proposed research sites and topic areas at a *Dissertation Bootcamp* where they are given feedback by potential Dissertation Advisors.

#### ***Dissertation Center***

Prior to Research Preparation courses, doctoral students are given access to the *Dissertation Center* in *eCollege*. The *Dissertation Center* is a resource for doctoral students which includes templates for dissertation deliverables, APA guidelines, access to the DIA and DSc Dissertation Handbooks and completed dissertations of UoF alumni.

#### ***Dissertation Development Support***

On an as needed basis, the Director of Doctoral Advising conducts a writing workshop for doctoral students needing additional guidance on the development of dissertation deliverables. Doctoral students may also attend webinars presented by members of the Candidacy Committee who describe dissertation requirements and the dissertation approval process.

#### ***Dissertation Handbook***

The *University of Fairfax Dissertation Handbook* has been developed as a resource to help guide doctoral students through the dissertation process, from identifying a feasible field research dissertation topic to producing a defensible dissertation. Students have access to this document in the *Student Information Center* and in the *Dissertation Center*.

#### ***Dissertation Project Plan***

To ensure that students make steady progress towards the completion of their dissertations, the University has developed the *Dissertation Project Plan* (DPP). This plan consists of a series of deliverables students produce while they are enrolled in research methods, research preparation and dissertation development courses.

## **ACADEMIC POLICIES AND PROGRAM EXPECTATIONS**

### **ACADEMIC CALENDAR**

The University's Academic Calendar is published for each calendar year. The Academic Calendar is posted in the *Student Information Center* in *eCollege*.

### **ACADEMIC TERM**

The University operates on a semester-based schedule with three semesters per calendar year (trimester). The academic terms (Spring, Summer and Fall) are each 16 weeks in length and consist of two eight-week course sessions (Course Session I and II). Course sessions begin on the first Sunday of January, March, May, July, September and November, unless changed due to major holidays.

### **ACADEMIC YEAR**

The academic year consists of two academic terms, or 32 weeks. The University offers continuous enrollment, whereby a student may begin a program of study in any course session. The course session in which a student starts a program of study determines the student's academic year.

### **ACADEMIC CREDIT POLICY**

The curriculum at the University of Fairfax is based on a semester hour of credit. Assignment for credit must be equivalent and conform to commonly accepted and traditionally defined units of academic measurement. The University assigns one semester credit for 15 hours of academic engagement and 30 hours of preparation, a formula commonly referred to as a Carnegie Unit of Credit.

Unless otherwise noted, courses offered at the University are three semester credits. Each course, therefore, must meet student workload requirements of 45 hours of academic engagement and 90 hours of preparation. This academic effort may consist of contact hours, learning activities and assignments used in meeting individual course requirements.

### **ACADEMIC INTEGRITY POLICY**

The principles of academic integrity encompass standards of honesty and truth. Each member of the University has a responsibility to uphold the standards of the community and to take action when others violate them. Faculty members have an obligation to educate students about the standards of academic integrity and to report violations of these standards to the Dean of Academic Systems, Services, and Assessment (DASSA).

The University of Fairfax regards academic honesty and scholarly integrity to be essential to the education of our students. Violations are not tolerated. Students may be dismissed for violation of the University of Fairfax standards of academic conduct. Detailed explanations of violations and procedures are available in the *Student Handbook* and *Faculty Handbook*.

## **PROFESSIONAL CONDUCT POLICY**

Students are expected to abide by all public laws and generally accepted professional standards, to comply with all regulations and policies of the University, and to conduct themselves professionally when interacting with fellow students, faculty and staff.

The University of Fairfax reserves the right to place on probation or dismiss students who engage in unsatisfactory conduct such as dishonesty; failure to adhere to rules and regulations; destruction or theft of property; participation in activity that impinges on the rights of others; or possession or consumption of alcoholic beverages or illegal drugs at any time on the school premises. In any case of probation or dismissal students may appeal.

## **STUDENT RIGHTS AND RESPONSIBILITIES**

The University has established policies that govern student, faculty, and staff behavior. Students are required to be familiar with these policies and adhere to them. These policies are published in the *Student Handbook* and include:

- Academic Freedom
- Academic Records Policy
- Grievance Policy
- Harassment Policy
- Intellectual Property Policy
- Nondiscrimination Policy
- Copyright Policy
- Drug and Alcohol Policy
- Confidential Information Policy
- Research Practices Policy

## **ATTENDANCE**

Attendance in the first week of the course is evidenced by participation in the discussion threads. Registered students who do not participate (i.e., post to discussion threads) by Saturday of Week 1 are dropped from the course and receive a grade of “DR”.

## **PARTICIPATION**

The University’s learning management platform (*eCollege*) enables students to conveniently access coursework. Students are required to participate by posting to asynchronous threaded discussions and by attending online synchronous class sessions (*SyncSessions*) as scheduled. Participation is a graded component in the calculation of the course grade. In addition, students are encouraged to participate each week in online chat room sessions facilitated by the professor in each course.

## **TECHNOLOGY REQUIREMENTS**

Students must have personal access to a Windows-enabled computer with a minimum of 512 MB RAM, high speed internet connectivity, and the appropriate office suite of software to support word-processing, presentation development and spreadsheet capabilities. In addition, a web-cam and microphone/headset are required.

## **STANDARDS OF ACADEMIC PROGRESS**

Academic progress is evaluated at the end of each term. Students must demonstrate satisfactory academic progress by meeting the University's established standards for academic progress in each of three areas:

- Cumulative grade point average
- Maximum coursework allowed
- Completion rate

### **Cumulative Grade Point Average**

Students must maintain a minimum cumulative grade point average (CGPA) of 3.0 in order to remain in good academic standing.

### **Maximum Coursework Allowed**

Students may attempt no more than 1.5 times the number of credit hours associated with the program in which they are enrolled. A student who exceeds this maximum and has not graduated may be dismissed.

### **Completion Rate**

Students must earn credit toward graduation at a pace (rate of progress) that ensures successful program completion within the maximum coursework allowance. At least one course must be completed during an academic term in which they are enrolled. The completion rate is the ratio of credit hours passed to credit hours attempted. A student must maintain a minimum completion rate of 67 percent of attempted credit hours.

## **ACADEMIC STANDING**

### **Good Academic Standing**

Academic standing is evaluated at the end of each course session. Students enrolled in a degree program are considered to be in good academic standing if: they maintain a minimum CGPA of 3.0 or higher, have attempted no more than 1.5 times the number of credit hours associated with their designated program, and have maintained a completion rate greater than 67 percent of attempted credit hours.

---

### **Academic Warning**

Students who fail to maintain a status of good academic standing are placed on academic warning. Specifically, students who receive a grade of “F” in any course session or whose CGPA is below 3.0 in a given academic term are placed on academic warning.

Students placed on academic warning must obtain academic advising from the Dean and are given an academic plan for returning to the status of good standing.

### **Academic Probation**

Academic probation constitutes conditional permission for students to continue to enroll in courses. Students failing to return to a status of good standing or whose CGPA remains below 3.0 for consecutive academic terms (i.e., more than one academic term) are placed on academic probation.

Students on academic probation must obtain academic advising from the Dean and are given an academic plan for returning to the status of good standing. A student placed on academic probation may submit a written appeal of the decision to the Academic Affairs Committee.

### **Academic Dismissal**

A student may be dismissed from an academic program if one or more of the following apply:

- the student has failed to make progress toward returning to the status of good standing within the timeframe identified in the academic plan set forth by the Dean;
- the student has exceeded the maximum coursework allowed for the program in which they are enrolled;
- the student has failed to meet rate of progress standards established by the University;
- the student has committed an act of substantial academic and/or professional misconduct in violation of the Professional Conduct Policy described in the University of Fairfax Student Handbook;
- the student has exceeded the time limit for completion of their designated degree program, unless the Registrar has issued written approval for a time extension.

A student who is dismissed may submit a written appeal of the decision to the Chief Academic Officer (CAO).

### **COMPUTING A CUMULATIVE GRADE POINT AVERAGE (CGPA)**

A cumulative grade point average (CGPA) summarizes a student’s academic performance in all coursework completed. The CGPA is also used in determining the student’s academic standing. To compute the CGPA, the letter grade for each course is first converted to a grade point value (GPA Value as noted under Grading Scale) and multiplied by the number of credits designated for the course to determine GPA Points (GPAPTS) earned. GPAPTS are displayed on the transcript for each course. To determine the CGPA, the sum of all GPAPTS earned is divided by the total number of credits attempted. Courses assigned an “I,” “DR,” “W,” “P,” “NP” or “AUD” are not used in computing a grade point average.

## GRADING SCALE

The University uses a grading scale based on letter grades as outlined below.

Grade	GPA Value	Academic Designators	
A	4.0	Incomplete	I
A-	3.7	Drop	DR
B+	3.3	Withdrawal	W
B	3.0	Progress	P*
B-	2.7	No Progress	NP*
C+	2.3	Audit	AUD
C	2.0		
F	0.0		

\*In dissertation courses, the grades of “P” and “NP” are assigned instead of letter grades.

### Incompletes

The grade of Incomplete (“I”) is granted in cases where students in good standing are in need of additional time to complete course requirements due to circumstances such as work-related travel or health. If the remaining coursework has not been submitted within four weeks of the end of the term, the “I” automatically becomes a grade of “F” unless an extension is granted by the Dean.

### Withdrawals

Students who withdraw from a course are given a grade of “W”. Students who do not submit all coursework and do not officially withdraw from a course, or do not receive approval for an Incomplete, may receive a grade of “F”.

### Audited Courses

Students who wish to audit a course must receive prior approval from the Dean and adhere to the same attendance requirements as all other class members. Although audit students are not required to complete projects, they may do so. The audit designator (“AUD”) appears on transcripts and signifies neither credit nor grade.

A previously audited course may be taken for credit at a later date. In addition, a student may audit a course previously taken and passed. Tuition and fees apply to all audited courses.

### Repeated Courses

Students must repeat a course for which a grade of “F” has been assigned. Students may repeat courses within their program of study (at the tuition rate in effect at the time they repeat) in order to improve their CGPA or to enhance their understanding of course material, with permission from the Dean. Only the highest grade earned is included in calculating the CGPA. A record of all registrations remains on the transcript, with the notation Repeat. Credit for the same course is awarded only once. Students may repeat a single course no more than three times unless approved by the Dean.

---

## **PROGRAM MODIFICATIONS**

### **Course Substitutions**

Upon written request to the Dean, students may receive approval to substitute an elective course for a core or specialization course if the student has requisite knowledge of the content of the course being replaced. Documentation such as academic transcripts, a detailed job description, resume and/or evidence of a relevant license or certification may be required.

### **Transfer of Course Credits**

A maximum of nine semester credits may be transferred into a degree program. No transfer credit will be applied to programs of study where a doctoral student has been granted advanced standing. The University does not award academic credit for non-academic experience.

To receive transfer credit for a course, the following criteria must be met:

- The student must have taken the course for graduate credit as part of a degree or graduate certificate program from an accredited institution;
- The course taken was equivalent to the University of Fairfax course in content, level, and credit hours;
- The student earned at least a grade of “B” (courses taken on a pass/fail basis are not eligible for transfer); and
- Information Security courses must have been completed within the five years preceding initial enrollment at the University of Fairfax.

Students and graduates should note that when seeking to transfer credits to another educational institution, the receiving institution has full discretion as to which credits are transferable.

### **Program Modifications for Dual Degree Seekers**

Students seeking consecutive degrees (MSISM/DIA or MSISM/DSc) who have a previously earned Master’s degree in an Information Security related discipline from an accredited institution may petition to transfer up to 18 credits toward the MSISM degree. In cases where the petition is approved, upon completion of the required courses, the MSISM degree may be awarded without a specialization.

## **STUDENT IDENTITY VERIFICATION**

Each student must submit a digital image of his/her government issued ID card to a secure Dropbox in the *Student Information Center*. The images are used by faculty members/proctors to validate each student’s identity during proctored exams. Students establish web-cam sessions during the proctored exams so that the proctor may compare the student appearing on-camera with the image on the previously submitted ID card to verify that they are the same.

---

## **PROCTORED EXAMS**

### **Master's Degrees**

For the MSISM degree program, proctored oral examinations are conducted during the last SyncSessions of IA7020 and IA7030 to assess learning outcomes related to the evidence-based analysis and assessment of best practices associated with the 10 domains of Information Security; during the last SyncSession of RM6000 to assess learning outcomes related to the development of secondary research skills used in the analysis of issues relevant to Information Security practitioners; and during the last SyncSession of IA9200 to assess learning outcomes which integrate the concepts introduced in the core courses of the program. The proctored exams are based on the course activities and deliverables completed during these courses.

For the MSEM degree program, proctored oral examinations are conducted during the last SyncSessions of EM7020 and EM7030 to assess learning outcomes related to the evidence-based analysis and assessment of best practices associated with enterprise management; during the last SyncSession of RM6100 to assess learning outcomes related to the development of secondary research skills used in the analysis of issues relevant to enterprise managers; and during the last SyncSession of EM9200 to assess learning outcomes which integrate the concepts introduced in the core courses of the program. The proctored exams are based on the course activities and deliverables completed during these courses.

### **Doctoral Degrees**

For the doctoral degree programs, proctored oral examinations are conducted during the last SyncSessions of IA7020 and IA7030 to assess learning outcomes related to the evidence-based analysis and assessment of best practices associated with the 10 domains of Information Security; during the last SyncSession of RM6000 to assess learning outcomes related to the development of secondary research skills used in the analysis of issues relevant to Information Security practitioners; during the last SyncSession of RM8500 to assess learning outcomes associated with the concepts and foundations of applied field research; and at the oral defense of the doctoral dissertation (when the DIA candidate is enrolled in DST8130 or when the DSc candidate is enrolled in DST8540) to assess research competencies.

## **CONTINUOUS ENROLLMENT/GOVERNING RULES**

Students are governed by graduation requirements in effect at the time of initial enrollment, provided their enrollment has been continuous. Continuous enrollment is interrupted when a student is not enrolled for more than one academic term. For each interruption of continuous enrollment, students are governed by graduation requirements and policies in effect at the time of resumption of enrollment. Students who have not registered for a course for a year or more must re-apply for admission to the University.

## **TIME LIMIT FOR COMPLETION**

Doctoral students are given up to seven years from the date of initial enrollment to complete degree requirements. Students enrolled in the MS degree program are given up to five years from the date of initial enrollment to complete degree requirements. However, students may petition the Registrar to receive an extension.

## **GRADUATION REQUIREMENTS**

In the academic term following a student's last course, the Registrar certifies that the student has completed all requirements for graduation. If certified, a diploma indicating the degree and applicable specialization(s) is issued.

### **All Graduates**

In order to graduate, all students must:

- complete the minimum number of credit hours designated for the chosen degree program.
- satisfy all program requirements including completion of courses for the chosen degree and specialization(s).
- achieve the minimum cumulative GPA designated for the chosen degree program.
- pay all tuition and fees and fulfill all other administrative obligations to the University of Fairfax.

### **Graduates of the Doctoral Program**

In addition to the above, doctoral candidates must produce and successfully defend an approved dissertation as specified in the University of Fairfax Dissertation Handbook for their designated degree.

### **Alternate Degree Award for Doctoral Students**

Doctoral students who have completed a minimum of 36 semester credits of a University of Fairfax doctoral program, but wish to discontinue doctoral studies, may be awarded an MSISM degree with a specialization in *Information Security Research*. These students may re-apply to a University of Fairfax doctoral program at any time. Previously earned credits at the University may be applied towards completion of the doctoral degree upon reentry.

## **TRANSCRIPT REQUESTS**

Transcripts are issued by the Registrar upon receipt of a signed *Transcript Request Form* along with fee payment. Transcripts will not be issued to any student who has an outstanding obligation to the University. The *Transcript Request Form* is available in the *Student Information Center* and on the University website.

## FINANCIAL INFORMATION<sup>15</sup>

### TUITION

Tuition is \$895 per semester credit.

### FEES

<i>Description</i>	<i>Rate</i>
Application	\$75
Graduate Certificate Award	\$200 per certificate
Graduation	\$400 <sup>16</sup>
Late Registration	\$25 per registration period
Returned Check/Declined Credit Card	\$25 per occurrence
Student Services	\$50 per course session
Technology	\$125 per course
Transcript Request	\$5 per transcript

### SPECIAL SERVICES FEES

<i>Description</i>	<i>Rate</i>
Advanced Standing Evaluation	\$895
Dissertation Quality Review	\$895
Registration ( <i>One Time</i> )	\$200
Transfer Credit	\$75
Review Seminar Fee	\$2695

#### Advanced Standing Evaluation

Applicants to the *Doctor of Science in Information Assurance (DSc)* who seek advanced standing status are charged an advanced standing evaluation fee.

#### Dissertation Quality Review

To ensure that all dissertations meet University standards, each dissertation must undergo a *Quality Review*, prior to defense. Doctoral candidates are charged a fee for each *Quality Review*.

<sup>15</sup> Tuition, fees and financial policies are subject to change without notice.

<sup>16</sup> This fee is reduced by \$150 for degree seekers who have earned multiple graduate certificates.

### **Registration**

Students who drop/withdraw from a course after the five-day cancellation period are charged a registration fee. This fee is charged to a student only once during a degree or certificate program.

### **Review Seminar Fee**

This fee is charged for enrollment in an approved certification exam review seminar.

### **Student Services**

The Student Services Fee helps to support access to the *Library Portal (LP)* and ongoing enhancements to the LP, including digital data base subscriptions and Inter-Library Loan, as well as tutorials conducted by the Online Librarians. This fee also helps to support University sponsorship of student membership in the *Information Systems Audit and Control Association (ISACA)* which provides student access to peer-reviewed journal articles.

### **Technology**

The Technology Fee helps to support access to the full suite of capabilities of the online learning platform. These include *ClassLive Pro* as well several repositories of information for students, including the *Student Information Center (SIC)*, the *Dissertation Center (DC)* and the *Graduation Center (GC)*.

### **Transfer Credit**

Students who transfer credits to UoF from another institution are charged a transfer credit processing fee.

## **FINANCIAL POLICIES**

### **Add/Drop Period**

Students may add or drop a course during the Add/Drop Period which ends Saturday of Week 1 of the course session. New students, however, are strongly encouraged to complete registration no later than Wednesday of Week 1. Course registrations beyond the Add/Drop period require approval by the Dean. Registered students who do not attend a course (as evidenced by course participation) by Saturday of Week 1 will be administratively dropped from the course and will receive a grade of “*DR*”.

Students with mitigating circumstances may submit an appeal to the Registrar for re-entry into a course, no later than Wednesday of Week 2. The appeal will be granted or denied based on factors such as previous history of non-attendance, academic performance and the circumstances presented by the student.

### **Withdrawals**

Students who wish to withdraw from a course after the Add/Drop Period must notify the school by Saturday of Week 7 of the course. Simply ceasing to attend a course does not constitute a withdrawal. Students who withdraw from a course after Week 1 receive a grade of “*W*”.

Students must notify the school if they wish to withdraw from a program. Any outstanding balances at the time of program withdrawal require payment in full after refund calculation.

## Refunds

A student who cancels in any manner within five days of signing a Course Enrollment Agreement will receive a 100% refund of all monies paid, within thirty (30) days of notification.

Students who withdraw from a course after the Cancellation Period receive refunds on a percentage basis according to the student's withdrawal date in relation to the most recent period of enrollment for which the student has paid. In addition, students are assessed a non-refundable "registration fee" of \$200, *only once* during the student's program of study. Any refunds due students will be received within 30 days of notification of drop/withdrawal as shown below:

<i>Date of Drop/Withdrawal</i>	<i>Refund Due</i>
<i>Prior to Week 1*</i>	<i>100%*</i>
<i>Week 1</i>	<i>100% *</i>
<i>Week 2</i>	<i>80% *</i>
<i>Week 3</i>	<i>60%*</i>
<i>Week 4</i>	<i>40% *</i>
<i>Week 5</i>	<i>20% *</i>
<i>Weeks 6-8</i>	<i>0%</i>

*\*Weeks are defined as Sunday – Saturday.*

## FINANCIAL ASSISTANCE

### Program and Lifetime Maximums

Students qualify for a maximum level of financial assistance based on program of study, merit, and/or financial need. The total amount awarded to a student may have multiple sources of financial assistance allocated against that maximum.

### FORMS OF FINANCIAL ASSISTANCE

#### Military Spouse Career Advancement Accounts (MyCAA)

The University has met Department of Defense (DoD) eligibility requirements to participate in the *MyCAA Financial Assistance Program*. This program provides up to \$6000 in financial assistance to military spouses who are pursuing degree programs leading to employment in portable career fields. Spouses of Active Duty members of the DoD and activated members of the National Guard and Reserve Components are eligible. Eligible spouses can establish a *MyCAA* account by visiting <https://aiportal.acc.af.mil/mycaa/>.

## **Employer Tuition Reimbursement/ Direct Billing**

Many employers reimburse their employees for tuition. Students should contact their supervisor or employee benefits office to determine if tuition reimbursement is available. For those students whose companies finance their education, a direct billing arrangement between the employer and the University may be arranged.

## **Scholarships, Fellowships and Loans**

The University offers multiple sources of tuition financing for eligible students, including fellowships, scholarships and loans. Fellowship and scholarship awards are based on merit and need and vary based on the availability of funds each term. Students must remain in good academic standing and meet financial obligations to the University in order to continue to receive fellowship or scholarship disbursements.

### **Scholarships**

#### *Aladdin*

The University established the Aladdin Scholarship Fund on behalf of *Aladdin Systems* in recognition of its support for the University of Fairfax.

#### *Cybersecurity Best Practices*

The University established the *Cybersecurity Best Practices Scholarship* to support and encourage cybersecurity professionals to obtain the CISSP certification. This scholarship applies to approved certification exam review seminars..

#### *Government Security News (GSN)*

The University established the *GSN Scholarship Fund* in conjunction with GSN, a resource for up-to-date information serving a community of over 40,000 security professionals.

#### *Information Security Certification*

The University established an *Information Security Certification Scholarship Fund* to assist degree-seeking applicants who hold selected, recognized information security certifications such as CISSP, CISM, and CISA prior to enrollment.

#### *NSA Certification*

The NSA has validated the University of Fairfax curriculum as mapping 100% to the Committee on National Security Systems (CNSS) National Standards 4011 and 4012. To support and encourage cybersecurity professionals to obtain these certifications, the University has established the *NSA Certification Scholarship Fund*.

### **Research Fellowships**

The University has established several fellowship funds to support needed cybersecurity research. These funds include the *FISMA Fellowship*, the *HIPAA Fellowship*, the *Cybersecurity Policy Fellowship* and the *Cyber Intel Fellowship*.

Preference is given to individuals who demonstrate a capability and motivation to undertake doctoral studies in the DIA or DSc degree programs. Fellowship awards are based on merit and/or need. Students must remain in good academic standing and meet financial obligations to the University in order to continue to receive fellowship disbursements.

### **Educational Loans**

The University has arranged for educational loans to be made available to students from:

#### ***Sallie Mae***

Sallie Mae offers graduate students educational loans. To obtain an application, go to: [www.salliemae.com](http://www.salliemae.com) and click on *Sallie Mae Smart Option Student Loan* or call 888.2.SALLIE (725543).

#### ***Institutional Financing***

The University offers institutionally supported loans and payment plans for students based on merit and/or need. To obtain an application, email the Financial Services Coordinator at [studentfinance@ufairfax.net](mailto:studentfinance@ufairfax.net).

## COURSE DESCRIPTIONS

### CORE COURSES

#### *Information Security Degrees*

##### **IA7020 Information Security Systems and Organizational Awareness**

In this course, students utilize a subset of five of the ten domains of the (ISC)<sup>2</sup> Common Body of Knowledge (CBK) in information security as a framework to critically analyze security awareness issues and to evaluate best practices in implementing security systems within the enterprise. (3 credits)

##### **IA7030 Legal and Ethical Practices in Information Security**

In this course, students utilize a subset of five of the ten domains of the (ISC)<sup>2</sup> Common Body of Knowledge (CBK) in information security as a framework to critically analyze ethical decision-making and to evaluate the best practices employed in security operations planning and management. (3 credits)

##### **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)

Prerequisites: IA7040, IA8010, PM8100

##### **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***

### **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)*

### **PM8000 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)*

### **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)*

Prerequisites: *EM7040, EM8010, PM8000*

---

## **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**

In this course, students explore advanced techniques and tools for identifying and categorizing vulnerabilities which allow penetration of networked systems and environments. *(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)*

### **IA8125 Information Security 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 for the enterprise. *(3 credits)*

### **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)*

### **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)*

### **IA8210 Risk Management and Compliance**

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

---

## ELECTIVE COURSES

### **IA9310 Research Topics in Certification and Accreditation**

In this course, students independently explore emerging trends in procedures, activities, and management structures utilized to certify and accredit information systems for the protection of the data and systems. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

### **IA9320 Research Topics in Security Policy and Governance**

In this course, students independently explore emerging security policies, standards and regulations and their impact on the enterprise. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

### **IA9330 Research Topics in Risk Management and Compliance**

In this course, students independently explore emerging trends with respect to compliance processes which address the regulatory requirements that drive the need for risk analysis within the enterprise. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

### **IA9340 Research Topics in Continuity Planning and Disaster Recovery**

In this course, students independently explore emerging strategies for Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) activities. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

### **IA9350 Research Topics in Risk and Vulnerability Assessment**

In this course, students independently explore leading tools, technologies and methodologies used in identifying, prioritizing and mitigating information system threats and vulnerabilities. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

### **IA9360 Research Topics in Intrusion Detection and Prevention Methods**

In this course, students independently explore emerging trends in attack methods, detection technologies and tactical countermeasures employed in protecting enterprise resources. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

### **IA9370 Research Topics in Security Architecture Design Methodologies**

In this course, students independently explore the critical factors influencing the selection and implementation of security solutions which support a “defense-in-depth” security architecture. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

### **IA9380 Research Topics in Wireless and Mobile Security**

In this course, students independently explore emerging topics such as risks and vulnerabilities, assessment methods and standards associated with wireless and mobile technologies. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

### **IA9390 Research Topics in Forensic Evaluation**

In this course, students independently explore emerging topics related to electronic discovery and analysis of cyber evidence. Students produce a research paper which demonstrates knowledge of the topic area, mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. *(3 credits)*

---

## RESEARCH COURSES

### *Comprehensive Exam Courses*

#### **CEX8220 Security Program Strategies and Implementation (Level I)**

In this course, students independently explore the components of a security program for an enterprise and develop a strategy for its implementation. Students must complete a written exam paper which demonstrates mastery of literature-based research skills and American Psychological Association, 6<sup>th</sup> edition (APA) format and citation requirements. (3 credits)

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

In this course, students independently 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)

#### **CEX8240 Strategic and Technological Trends in Information Security (Level I)**

In this course, students independently 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)

#### **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)

### *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. (3 credits)

#### **RM6100 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)

#### **RM8200 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)

#### **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)

---

**RM8500 Research Foundations for Information Security Practitioners**

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)

**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: RM8500

**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 or problem assessment. (3 credits)

**RM9200 Designing Solutions to Information Security Problems**

In this course, doctoral students enrolled in the DIA program continue to evaluate the feasibility of their proposed research site and the potential solutions to be studied. Students present their proposed project at the *Dissertation Bootcamp* at the end of this course. (3 credits)

**RM9250 Building a Knowledge-Base in the Information Security Discipline**

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)

***Research Preparation Courses – DIA***

**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 Identification of Evidence-Based Solutions**

In this course, students conduct a literature review in Information Security and other relevant bodies of research to identify a proposed solution to the business problem. Using this literature review, they present support for the selection of the proposed solution and identify criteria to be used in assessing its feasibility. (3 credits)

**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 the methodology to be utilized in the proposed project in the *Feasibility Study Specification* (FSS) which is the final course deliverable. (3 credits)

**RES8140 Continuing FSS Development**

Doctoral students requiring additional time to produce an approved *Feasibility Study Specification* (FSS) enroll in this course until the document is approved by the Candidacy Committee. (1 credit)

---

## ***Research Preparation Courses – DSc***

### **RES8510 Research Topic Rationale**

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)

Prerequisite: *RM9250*

### **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. (3 credits)

### **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)

### **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 credit)

### **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)

### **RES8560 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)

### **RES8570 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)

### **RES8580 Continuing RDS Development**

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 credit)

## ***Dissertation Development Courses-DIA***

### **DST811X Feasibility Testing and Planning**

In this course, doctoral candidates implement the approved feasibility study by collecting and analyzing data relevant to the criteria identified for the adoption, integration and implementation of the proposed improvement to professional practice. (1-6 credits)

Prerequisite: *Approved FSS*

### **DST8120 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)

### **DST813X 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*

***Dissertation Development Courses-DSc***

**DST851X 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. *(1-6 credits)*

Prerequisite: *Approved RDS*

**DST852X Data Analysis and Findings**

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

**DST8530 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)*

**DST854X 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*

## **PROFESSIONAL DEVELOPMENT COURSES**

### **IC7000 (ISC)<sup>2</sup> Official CISSP Review Seminar**

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

---

## FACULTY

To ensure that the University of Fairfax accomplishes its mission to provide high quality practitioner-oriented graduate programs, the University utilizes an expert professional faculty who are senior practitioners in information security and/or field research methods. These experienced professionals help students to remain current with accelerating trends and evolving issues in Information Security, Information Assurance and Enterprise Management so that they may rapidly apply what they learn to their jobs and continue to advance their careers.

**Michael Aisenberg, JD** is a Principal in the Information Security & Privacy practice of MITRE Corporation's Defense and Intelligence FFRDC where he provides strategic policy advice to federal agencies managing the security of the nation's most sensitive networks and databases. Mr. Aisenberg also serves as the Chairman of the American Bar Association's Information Security Committee. His prior positions include Special Assistant to the President of EWA Information and Infrastructure Technologies, Inc., a subsidiary of Electronic Warfare Associates and Corporate Director of Government Relations for VeriSign, Inc. where he managed the company's national security, intellectual property and trade policy portfolios, as well as leading the corporate standards policy function. As VeriSign's principal public policy liaison with the Administration and Federal agencies, he supported the CEO's participation in the prestigious Presidential National Security Telecommunications Advisory Committee (NSTAC) and chaired the International Task Force of the NSTAC Industry Executive Subcommittee. Mr. Aisenberg holds a JD from the University of Maine, School of Law and a BA from the University of Pennsylvania. Mr. Aisenberg is a member of the bar of the United States Supreme Court.

**Kenneth D. Bahn, PhD** has had a distinguished academic career spanning over 33 years. Dr. Bahn has served as the Director of the MBA program at James Madison University (JMU) where he championed the establishment of the first MBA program in Information Security in the U.S. In addition, he achieved NSA Center for Academic Excellence (CAE) status for the program. He has served on dissertation committees and chaired dissertation committees at VA Tech and University of Texas. His areas of research expertise are in children's consumer behavior, brand management, effective communications, environmental and ecological issues in marketing, nutrition, physical fitness and market segmentation. Dr. Bahn has conducted many seminars in the areas of Sales Training and Brand Equity Development. He has consulted for the Embassy of Ghana, the Expert-Witness Round Table Group and companies such as J.C. Penney, Inc., Dr. Pepper 7-Up Company and Dallas Water Utilities. He is the author of several books and has published extensively in refereed journals. Dr. Bahn holds a PhD in Business Administration with an emphasis in Marketing from the University of Utah, and both an MS in Marketing and a BS in Business Administration from California State University, Long Beach.

**Alden S. Bean, PhD** served as the Executive Director of the Center for Innovation Management Studies (CIMS) at NC State University. Before joining CIMS, Dr. Bean held the Wm. R. Kenan, Jr. Chair in Management and Technology in the College of Business and Economics at Lehigh University. Prior to his Lehigh appointment, Dr. Bean was the Director of the Policy Research and Analysis Division of the National Science Foundation. He also served on the faculties of the University of Cincinnati, the State University of New York at Albany and Northwestern University. Dr. Bean's research involves studies of patterns in the organization and funding of U.S. industrial R&D activities, the role of technology in U.S. firms' corporate strategy, and technological innovation and productivity growth in U.S. firms. He has authored numerous articles on research management and science and technology policy. Dr. Bean earned his PhD from Northwestern University in R&D Management and Organization Theory.

**Dominic Boamah, PhD** is a consultant on course development for the Distance Learning Center of the Ghana Institute of management and Public Administration. Previously, he served as Software Test, Certification and Compliance Lead at Nokia, Inc. and TapRoot Systems. Dr. Boamah has had extensive online teaching experience. His presentations include *Surviving as an Online Learner*. Dr. Boamah earned his PhD in Organization and Management with a specialization in Information Technology Management from Capella University. Dr. Boamah holds an MS in Economics and Business Administration from University of Jyvaskyla, Jyvaskyla, Finland and a Diploma in Data Processing from the University of Science and Technology, Kumasi, Ghana.

**Wayne Boone, PhD** is a retired senior Canadian Forces Military Police Officer with over twenty-one years of experience in the provision of effective and appropriate Information System security and over twenty-nine years of experience in the provision of Corporate Security, Critical Infrastructure Protection (CIP) and Business Continuity Planning (BCP) for sensitive private and government activities, in both static and deployed environments. Currently he serves as an Assistant Professor at the Norman Paterson School of International Affairs at Carleton University, Ottawa, Ontario. Dr. Boone's research interests are security program governance and leadership, threats to assets (including terrorism and natural hazards), and security policy. He holds a PhD in Information Assurance from the University of Fairfax, an MA in War Studies and a BA in Political Science, both from the Royal Military College, Kingston Ontario.

**Certifications:** *CD, CISSP, CPP, CBCP, CISM, PCIP*

**Khanh P. Bui, PhD** has over 20 years of experience in information technology (IT) and IT security. Currently she is a Senior Security Engineer at Northrop Grumman where she has supported the information security needs of customers including the FAA, DHS and the DOD. Dr. Bui was designated a TRW Doctoral Fellow and earned a PhD in Information Technology from George Mason University. She earned an MS in Computer Science from George Mason and a BS in Computer Science from the University of Washington, Seattle.

**Certifications:** *CISSP, ISSEP, CISA, CAP, Six Sigma Black Belt*

**Bryan S. Cline, PhD** is the VP, Common Security Framework Development and Implementation for the Health Information Trust Alliance and serves as the Chief Information Security Officer (CISO). He previously served as Director, Information Security for Catholic Health East, a multi-institutional health system consisting of 34 acute care hospitals and numerous other health care facilities in 11 eastern states stretching from Maine to Florida. He has also served as the Chief Information Security Officer and Director of Information Security Risk Management for The Children’s Hospital of Philadelphia and as the Technical Director of Information Assurance (IA) Services for QinetiQ North America Defense Solutions. Dr. Cline has more than 25 years of experience in information systems, 10 years of which were in information systems security management and engineering for the DoD and NATO. He has presented and participated in panels at Techno Security, Techno Forensics; Secure World, SC World Congress, and the DoD Cyber Crime Conference. He has also published papers in professional journals such as the Information Systems Control Journal and Journal of Information Assurance and Security as well as in proceedings for INCOSE, IEEE and other conferences and symposia. He is the Founder and Coordinator of the Greater Philadelphia Chapter of the CSO Breakfast Club and member of the Club’s national Advisory Council. Dr. Cline holds a PhD in Information Systems with a concentration in IA Policy from the University of Fairfax, an MS in Industrial Engineering with a concentration in Operations Research from the University of Oklahoma and a BS in Mathematics from the University of Texas, Arlington.

***Certifications: CISSP-ISSEP, CISM, CISA, CPP, CAP (PM-II), ASEP, MCIAAT, NSA-IAM, and NSA-IEM.***

**Diane H. Dayson, PhD** has over 28 years of experience in management, leadership, change management, incident command, and strategic planning. She is a retired senior executive service (SES) level manager from the US Department of Interior, National Park Service. In her last position with the federal government she served as Executive Director/Superintendent of the Statue of Liberty/Ellis Island National Monuments. On September 11, 2001, Dr. Dayson had the responsibility of leading, managing, and making command decisions for the safety of employees, visitors, and park resources during the World Trade Center attacks. She has also served as Adjunct Professor at the New York University, Robert F. Wagner School of Public Service. Dr. Dayson holds a PhD in Public Policy and Administration from Walden University, an MS in Management from New York University, and BA in Education/American History from SUNY at Cortland.

**Lawrence W. Doe, PhD** has over 30 years of managerial and technical experience including positions as Senior Technical Director for General Dynamics (formerly Anteon Corporation), CIO for the University of Maryland Biotechnology Institute and Director of Information Systems for British Biotech. He has also consulted with numerous organizations on the use of business systems to enhance productivity. Dr. Doe earned his PhD in Industrial Engineering from Lehigh University, and his MS and BS in Chemistry from Lowell Technological Institute.

**Fadwa (Fay) Fayad, PhD** has over 20 years of experience in the IT and telecommunications field. Currently, she is a Senior Network Architecture Consultant for CSC in the Information Technology Infrastructure Solutions (ITIS) division of the North American Public Sector for Federal Contracts, where her expertise includes project and program management, engineering, integration, and the operation of large IT systems and networks. Prior to joining CSC, Dr. Fayad was an independent IT consultant and served as a Communications Engineering Officer and Program Manager with Infotech and IEI. In addition, Dr. Fayad has over 19 years of teaching and research experience at various institutions including the U.S. Department of Agriculture, George Mason University, the Fraunhofer Institute and Cairo University. She has authored and co-authored at least 12 published articles. Dr. Fayad earned her PhD in Microbiology jointly from Cairo University/Fraunhofer Institute. Her BS and MS were from Cairo University.

***Certifications: PMP***

**Norma Fleischman, PhD** has extensive experience in quantitative and qualitative evaluations, including the design of experimental and quasi-experimental evaluation studies, focus group research and interview protocols. Currently, Dr. Fleischman is a senior evaluator at the U.S. Department of Education's Rehabilitation Services Administration where she designs and oversees studies that assess the impact of the agency's programs and policies on providing effective and efficient services to persons who have disabilities. Previously, she served as Policy Analyst for the USDA, Food Safety Inspection Service. Dr. Fleischman has been the president of Washington Evaluators, a chapter of the American Evaluation Association, for the past five years. Dr. Fleischman earned her PhD in Education from the American University, her MPA from The George Washington University, and her BA from the University of Massachusetts, Amherst.

**Sheila Fournier-Bonilla, PhD** has over ten years of experience in marketing, teaching, research, program evaluation and assessment at institutions including Rensselaer Polytechnic Institute, Rutgers University, and Texas A&M University. Her teaching focus has included courses in quantitative modeling and business analysis, probability and statistics, quality improvement, and operations management. Dr. Fournier-Bonilla's research interests are in the areas of integrated quality planning, systems management, strategic management, and customer satisfaction. She has published in the areas of quality planning, quality improvement, and environmental assessment. Dr. Fournier-Bonilla holds a PhD in Interdisciplinary Engineering from Texas A&M University, and an MS and BS in Industrial Engineering from Rensselaer Polytechnic Institute.

**Jean E. Gordon, RN, DBA** has over 25 years of experience in operations management, human resource management and research supervision. Dr. Gordon is an established author of numerous peer reviewed articles and has co-authored many academic texts. In addition, she serves as a reviewer for the Journal of the American Academy of Business. Dr. Gordon earned her DBA with specializations in Human Resources and Marketing from Nova Southeastern University; she earned her MS in Human Resource Management from Nova Southeastern and her BSN from University of Miami.

**Steven M. Helwig, PhD** is a senior information assurance professional with over 20 years of experience in disaster recovery, organizational security, risk management, policy, compliance and network engineering. Currently he is the Senior IT Security Administrator for the Citizens Property Insurance Company. He served as the Executive Editor of the Compliance Authority Magazine. Dr. Helwig earned his PhD in Information Assurance from University of Fairfax, his MBA in Information Security from Salem International University, his MS in Information Systems from Capella University and his BS in Business Administration from University of Phoenix.

**Certifications:** *CISSP, NSA IAM/IEM*

**Crystal L. Keels, PhD** serves as the Program Manager for the Institute for International Public Policy (IIPP) at the United Negro College Fund Special Programs Corporation. She manages selected components of the IIPP Fellowship program including graduate school advisory functions, academic affairs, student affairs and program communications. Prior to joining IIPP, Dr. Keels served as a corporate editor in the private sector, and formerly served as an assistant editor for the magazine, *Diverse: Issues in Higher Education*. She is the recipient of the Cincinnati Editors Association 2000 Publications Competition First- Place Award for magazine writing/interviewing/profile and is the author of several published articles. Dr. Keels also served as Associate Instructor in English at Indiana University where she earned a PhD in English, as well as an MA in English and an MA in Journalism. She holds a BS in psychology from Xavier University.

**Aleksandar Lazarevich, PhD** is the Chief Engineer with the Department of Defense (DoD) Biometrics Program where he is responsible for all engineering, information assurance, and risk management activity on biometric systems used for forensic and intelligence support throughout DoD. Previously he served as Senior Research Engineer with the Defense Information Systems Agency's (DISA) Enterprise-Wide Systems Engineering office. In addition he served in the following capacities with DISA: Program Systems Engineer (PSE) for the Joint Enterprise Directory Service and the DoD Public Key Infrastructure (PKI) Program and senior engineer with the Joint Interoperability Test Command. As senior engineer, he directed major programs such as the Y2K certification effort for the Executive Office of the President, National Security Council, Office of Management and Budget, White House Communications Agency and Under Secretary of Defense (Logistics). His awards include: a letter of Commendation from the Deputy Under-Secretary of Defense for Logistics (May 2000); election to the *International Who's Who of Information Technology* (2001); DoD 30 year service Certificate (Jan 2004). Dr. Lazarevich earned his PhD in Information Technology, with an emphasis in Information Assurance and Computer Forensics, from George Mason University, an MSEE from the University of Arizona and a BSEE from the University of Wisconsin.

**Certifications:** *CISSP-ISSAP, CompTIA A+, MCP+I, CCNA, MCSE (NT & 2000)*

**David R. Lease, PhD** has over 25 years of technical and management experience in the information technology, security, telecommunications, and consulting industries. Currently, he is the Chief Solution Architect for CSC, a \$15 billion systems integrator. His recent projects include a \$2 billion IT security architecture redesign for a Federal law enforcement agency and the design and implementation of a secure financial management system for an organization operating in 85 countries. Dr. Lease is a writer and frequent speaker at conferences for organizations in the intelligence community, DoD, civilian Federal agencies, as well as commercial and academic organizations. Dr. Lease is also a peer reviewer of technical research for the IEEE Computer Society. Dr. Lease earned his PhD in Organization and Management from Capella University. His dissertation, *“Factors Influencing the Adoption of Biometric Security Technologies by Decision- Making Information Technology and Security Managers,”* was nominated for the 2006 Fredric M. Jablin Dissertation Award for its substantial insights and implications for leadership studies. Dr. Lease also earned an MS in Information Systems Management from the University of Southern California, an MBA in Finance from George Mason University, and a BS in Accounting from George Mason University.

**Certifications:** *CISSP, ISSAP, ISSMP, PMP, Six Sigma Black Belt, NSA-IAM, NSA-IEM, CHE, MCSE, CCNA, and ITIL.*

**Terrence V. Lillard** is an IT security architect and cyber forensics expert. He investigates and performs audits and assessments of computer intrusion, network and steganography in cybercrime and cyberforensics cases. Mr. Lillard has testified in US District Court as a Computer Forensics/Security Expert Witness. He has designed and implemented security architectures for various government, military, and multi-national corporations. Previously, he served in positions including Principal Consultant for Microsoft, IT Security Manager for the District of Columbia’s Government IT Security Team, and instructor for the Defense Cyber Crime Center’s (DC3) Computer Investigation Training Academy program. Mr. Lillard earned his MBA from Strayer University and his BSEE from Tuskegee University.

**Certifications:** *CISSP, CCE, SCNP, GIAC-GSEC, MCSE, CompTIA Network+ and I-NET+, CCNA*

**Craig E. Maddron, PhD** has over 15 years of experience in leadership positions in a wide range of areas, including business development, change management, project management, strategic planning and analysis, market research and product development. Currently, at General Dynamics, he serves as the Lead Specialist for Business Management at NOAA (National Oceanic and Atmospheric Administration and NESDIS (National Environmental Satellite, Data and Information Service) where his responsibilities include IT configuration management, project risk oversight and the development of strategic and operational IT plans. In the international arena, Dr. Maddron has been involved in implementing international educational initiatives for the technical professions. In addition, Dr. Maddron has 10 years of teaching experience in higher education and has published numerous articles. Dr. Maddron holds a PhD in Organizational Leadership from Capella University, an MBA in Financial Management from Southeastern University and a BS in Management from Park College.

**Carole Mourad, PhD** is a Security and Information Assurance specialist with over 10 years of multidisciplinary research, analysis and development experience in the security arena for both government and industry. Her experience includes cryptography, telecommunications, and computer and network security. She is an Expert in telecommunication security and vulnerability assessments on products to be approved on the APL (Approved Product List) for DISA (Defense Information Systems Agency). Currently she is a Subject Matter Expert (SME) Associate Level III in the Cryptologic Systems Group at Booz Allen Hamilton. Dr. Mourad earned her PhD in Electrical and Computer Engineering from the University of New Mexico and both her MS and BS in Electrical Engineering from Cornell University.

**J.G. Michael Parkes, PhD** has over 25 years of diversified experience in such areas as program and project management, threat and risk assessment and evaluation, environmental security and information technologies in Canada. Dr. Parkes founded Critical MAAS Technologies Inc. (CMTI), specializing in systems evaluation, and CONSILIUM, specializing in legal and regulatory impact analysis and risk management. In 2009, he founded Tusarvik Corp., a company focused on Arctic and northern development, planning and policy issues. Dr. Parkes has been a Visiting Research Professor at Carleton University and an Associate Professor at the Royal Military College, both in Canada. He holds a Professional Certificate in Critical Infrastructure Protection. Dr. Parkes earned a PhD in Geography from University College, University of London, England. He also holds an MA in Geography from University of Western Ontario, London, Ontario, Canada and a BA in Geography from Carleton University, Ottawa, Ontario, Canada.

**Laura Pogue, DM** is the Chief Executive Officer and President of Complete Consulting, Inc. which provides corporate online education and training for improved growth and profitability in the public and private sectors. Previously, she served as President of American Financial Consulting Group. Dr. Pogue is also a dedicated business educator, having taught business and management classes in the corporate, online, and traditional classrooms for the last decade. She has also served as Doctoral Program Mentor and Capstone Advisor at several Universities, including Jones International University. Over the last several years, Dr. Pogue has published and presented academic articles in the areas of leadership, management, executive compensation and international trade. Dr. Pogue earned a Doctor of Management degree in Organizational Leadership from the University of Phoenix and holds a BBA and MBA from the University of Michigan.

**Robert W. Robertson, PhD** has more than twenty years of management experience in the public sector in Canada, leading award winning organizations. Most recently, he served as the City Manager, City of Hamilton, Ontario, an organization with more than 8,500 employees and a budget in excess of one billion dollars. Previously, he served as Dean of the Bang College of Business and as Executive Director of the Center for Sustainable Urban Futures at the Kazakhstan Institute of Management, Economics and Strategic Research. He is an invited speaker at conferences world-wide. Dr. Robertson holds a PhD in Management and Organization from Stirling University, Scotland; a Master of Studies in Law in Public Policy/Administrative Law from Vermont Law School; an MPA in Local Government Management from Dalhousie University; an MA in Planning /Community Development from Eastern Kentucky University and a BS in Social Science/Geography from East Tennessee State University.

**Donald D. Rogers, PhD** has 30 years of management and technical experience. Currently, Dr. Rogers is an Information Assurance Engineer at Computer Sciences Corporation (CSC) and is assigned to the Defense Information Systems Agency. He has held Vice President and Director level management positions at Maximus, Research Development Institute, and Telos. More recently, he has served in hands-on network engineering positions at CACI, Integrated Communications Solutions, and CSC. Dr. Rogers has served as an Adjunct Professor at the University of Maryland (College Park) where he taught research methodology. He earned his PhD in Education from the University of Texas, Austin and his MEd and BS in Communications from the University of Illinois.

***Certifications: CISSP, CCSP, CCDP, CCIP, CCNP***

**Jeffrey Smith** has over 29 years of diverse experience in Information Technology and Security including analysis, implementation and testing of applications for both government and commercial organizations. Currently, he serves as a Federal Information Technology Compliance Officer. During his 23 year military career as a Naval Officer, he earned numerous military citations and awards including four Navy Commendation Medals for his work in Information Technology and Security. His positions included Chief Information and Security Officer onboard United States naval Ships and Shore Commands and Special Assistant for Communications on the Admirals Staff at Commander Mine Warfare Command. He is credited for bringing automated communications to the first Avenger class minesweeper. In addition, Mr. Smith serves as a security textbook reviewer for Thompson and Prentice Hall publishers. Mr. Smith holds an MS in Computer Technology from Nova Southeastern University and a BS in Human Resources from Park University. He is currently completing his doctoral research at Northcentral University.

***Certifications: CGISCP, CRISC***

**Gilbert N. Sorebo, JD** has worked in the information technology arena for more than fifteen years in both the public and private sectors. Mr. Sorebo currently serves as a Senior Information Security Analyst for SAIC where he assists government and commercial organizations to comply with legal and regulatory requirements including FISMA, GLBA and HIPAA. As an attorney, he specializes in information security, privacy, and electronic discovery. Mr. Sorebo has been active with the American Bar Association's Information Security Committee for several years and has contributed to publications relating to PKI, information security liability, and electronic discovery. He is a regular speaker at information security conferences on topics ranging from electronic discovery to Sarbanes-Oxley. Mr. Sorebo earned a JD from the Catholic University of America Columbus School of Law. He earned his MA in Legislative Affairs from George Washington University and his BA in Political Science from the University of Chicago.

***Certifications: CISSP, PMP***

**Janice M. Spangenburg, PhD** has had over 20 years of varied management experience including program management, budgeting, contract administration, and consulting for agencies such as DoD, U.S. Navy, Marine Corps and USPS. In addition, for the past 18 years she has held administrative and teaching positions in higher education. Her academic experience includes serving as Doctoral Mentor and Advisor on Dissertation Committees at institutions such as Capella University and Walden University. Dr. Spangenburg holds a PhD in Organizational Leadership from Regent University; an MA in Organizational Development from the Fielding Graduate School; an MS in Management from Troy University and a BA in Business Administration from St. Leo University.

**Leo J. Thrush** has 35 years of experience providing vision, leadership, and focus to complex enterprise information technology programs and networks spanning multiple countries and sites. His breadth of experience includes automation and telecommunications security, operations, and policy; space systems network security development, installation, and operation; security hardware and software requirements development, architectural planning and testing; financial and human resources management for enterprise IT operations; strategic communications operations, organizational structure and Certification and Accreditation. Mr. Thrush is the Chief Instructor for (ISC)<sup>2</sup> and lead trainer and mentor to the National Security Agency (NSA). His previous experience includes positions as Senior Advisor to the US Secretary of Defense (including the President and Senior Cabinet) and Chief of Operations, U.S. Space Command. His commercial training clients include HP, IBM, Microsoft, Cisco, Boeing, Raytheon, Lockheed Martin, and numerous others. He holds an MS in Administration from Central Michigan University and an MS in Strategic Resourcing from the National Defense University. He is a graduate of the Naval War College, the Air Command and Staff College, and the Army Command and Staff College.

**Certifications:** *CISSP, ISSEP, ISSMP, SSCP, PMP, CISM, GCSC, CAP*

**Mark J. Yader** has over 30 years of experience in senior management and technology positions. Mr. Yader currently serves as an independent IT and project management consultant. Previously, at GE he served as Director of E-Commerce Solutions for the Manufacturing Industry and led the product development of GE's Collaborative Supplier Extranet. While serving as Senior Architect for GE's Electronic Commerce Service Center, he led the design, development and deployment of new B2Bi technologies including Internet-based XML/edit messaging services. Mr. Yader received an MS in Computer Engineering from Stanford University and a BS in Applied Mathematics from Columbia University.

**Certifications:** *PMP, Six Sigma Green Belt, ITIL Foundation*

**Eric W. Yocam, PhD** has over 17 years of experience in leadership roles managing multiple global project teams. Currently, he serves as Group Program Manager in the IT division of Microsoft. His previous experience includes positions as Data Center Project Manager for Intuit Corporation and Technical Manager for HP. He holds a Certificate of Director Education, a nationally recognized designation for corporate directors confirmed in 2007 by the National Association for Corporate Directors (NACD) Corporate Directors Institute. Dr. Yocam earned a DBA from the University of Phoenix, an MS in Computer Science from California State University, an MS degree in Finance from Seattle University, an MBA from the University of San Diego and a BS in Computer Engineering from the University of the Pacific.

**Certifications:** *CISSP, PMP, CSDP, MPM, RBA*

---

## PROFESSIONAL ADVISORY COUNCIL

The *University of Fairfax Professional Advisory Council* provides guidance and feedback to the University to ensure that the University of Fairfax curricula continue to reflect current industry trends and continue to address the evolving needs of the Information Assurance community.

**Susan Baker** specializes in workforce development and educational initiatives, primarily in the Commonwealth of Virginia. She is passionate about the promotion and importance of Science, Technology, Engineering, and Math for students. Ms. Baker is a skilled trainer, marketer, and manager with a proven record of increasing organizational effectiveness by creative strategic planning and the development of strong public/private partnerships. Currently, Ms. Baker serves as Virginia's Statewide Base Realignment and Closure (BRAC) Workforce Project Manager, managing workforce and economic development initiatives, primarily at Fort Belvoir and Quantico Marine Base. In addition to statewide BRAC responsibilities, she also works as the Northern Virginia Executive Committee member of the regional Mid-Atlantic Regional Consortium (MARC), with colleagues from Maryland and Washington, D.C., to solve regional BRAC challenges. She has done extensive work in collaboration with the National Science Foundation's Scholarship for Service Program. Recently, she worked on the Information Technology Association of America's (ITAA) partnership project with DOL/ETA to develop the Information Technology (IT) Competency Model. Ms. Baker has served as a business advisor for President Bush's High Tech Growth Jobs Initiative and currently serves on the Advisory Board for Career and Technical Education for Governor Tim Kaine. Previously, Ms. Baker was Vice President of Workforce Development for the Northern Virginia Technology Council (NVTC), one of the largest and most nationally recognized councils in the United States. In this capacity, she worked closely with member company executives to attract top technology and engineering talent to the Northern Virginia region and to build educational pipelines of excellence for future workers. She also worked extensively with executives from IT companies, educational institutions, and federal, state and local officials on workforce and education public policy issues. Ms. Baker served on expert research panels for the National Science Foundation, the American Association for the Advancement of Science, Virginia Polytechnic Institute, and President Bush's Business Advisory Board for "No Child Left Behind." Ms. Baker earned a BA in Economics and French from Duke University. She is also a graduate of Leadership Fairfax – Class of 2001. She received an HR Leadership Award for Greater Washington in June 2003 and was recognized as the National Workforce Professional of the Year in November 2001.

**Christopher V. Feudo, DSc** has over 27 years of diversified experience in management, leadership, information systems and telecommunications engineering related to Information Assurance for Government and Commercial Systems. Currently he serves as Vice President and CTO of Edgewater Federal Solutions, providing consultative cybersecurity services to the National Nuclear Security Administration within the DOE. His prior position was President and CEO of Secureant. His previous experience includes positions as Director of Security and Privacy Professional Services for EDS and Senior Manager with Lockheed Martin Corporation. Dr. Feudo retired from the US Army where he served in Airborne, Ranger and Special Forces Units, culminating his military career as professor at the Defense Acquisition University. He has been the chairman of numerous subcommittees including the Internet Widespread Outage Committee within the President's National Security Telecommunications Advisory Committee, and was presented Vice President Gore's Hammer Award. Dr. Feudo earned his DSc in Computer Science from The George Washington University, his MS in Computer Science from the Naval Postgraduate School, and his BS in Engineering from the U.S. Military Academy, West Point.

***Certifications: DAWIA Program Manager, IAM.***

**Sarbari Gupta, PhD** has been active in the information security arena for over 20 years as an entrepreneur, executive, manager, consultant, system architect, researcher, and software engineer. She has a broad base of knowledge and experience in the areas of identity management, public key infrastructure, secure transactions, and system and network security. Dr. Gupta launched Electrosoft as an IT consulting business in 2001, and has been leading the organization on a variety of information security contracts for federal agencies (including NIST, GSA, NSA, Treasury, DHS, FAA, DEA, DOC, HHS) as well as commercial customers. She has helped to write several NIST standards and guidelines including FIPS 201 (Personal Identity Verification of Federal Employees and Contractors) and Special Pub 800-63-1 (Electronic Authentication Guideline). She has won several business awards including the 2008 *Outstanding 50 Asian Americans in Business Award* from the Asian American Business Development Center (AABDC); *25 Powerful Minority Women in Business* from the Minority Enterprise Executive Council in 2007; and *Fifty Influential Minorities in Business* from the Minority Business & Professionals Network in 2006. Dr. Gupta has authored over 20 technical papers/presentations in refereed conferences and journals, and holds four patents in areas of cryptographic key recovery and penetration analysis. She has participated in many standards activities, and has served as author/editor of ISO hashing standards and Open Group CDSA standards. She has been a Toastmaster since October 2007 and has achieved the Advanced Communicator Bronze (ACB) and Competent Leader (CL) levels. Dr. Gupta earned her PhD and MS in Electrical Engineering from the University of Maryland, College Park and a B.Tech degree in Electronics from IIT, Kharagpur, India.

***Certifications: CISSP, CISA, CAP.***

**Chrisan Herrod** is the Chief Information Security Officer for the University of Maryland, University College (UMUC) responsible for IT compliance, audit, risk management and business continuity. Prior to this position, she was Vice President for Business Development and Consulting at Compliance Spectrum where she was responsible for advising clients on creating and managing IT risk and compliance programs, forming business and strategic partnerships and driving strategic and thought-leadership/research activities for new products and services. Ms. Herrod has 20 years of private and public sector service; she is a retired federal government Senior Executive, having served as the Chief Security Officer at the Securities and Exchange Commission (SEC) where she was responsible for the Commission's information security, business continuity and IT auditing/ compliance programs. Her private sector experience includes positions as Director of Global IT Security at GlaxoSmithKline (GSK), one of the world's leading pharmaceutical companies. Prior to joining GSK, she was the Director of Information Security at Fannie Mae, a leading real estate, financial institution. She also served as a Senior Executive with the DoD as Program Director for the Information Security Program Office. Ms. Herrod speaks frequently at Compliance and Security conferences and symposiums and has written several articles and book contributions on Compliance and Security. Ms. Herrod received her MS in National Resource Strategy from the National Defense University and her BA in International Relations from Penn State University.

***Certifications: CISM, CISA, IAM***

**Hugh Kominars** has over 20 years of experience providing professional and technical advisory services to public and private sector clients across diverse industries including aerospace, defense, manufacturing, financial services and healthcare. Mr. Kominars is the VP of Partners, Alliances and Channels for Control Case, a provider of managed compliance services. Prior to joining Control Case, Mr. Kominars was Senior Manager in Ernst & Young's Advisory Services practice and has been with the firm for 11 years. His expertise includes technical and business risk analysis, internal controls design, business process analysis and redesign, information and security architecture design, data analysis, modeling and simulation, test and quality management, training curriculum development, and project management. Mr. Kominars leads the delivery of IT, security and operational governance, risk and compliance services for global clients headquartered in the Mid-Atlantic Area. The scope of work encompasses domestic and foreign subsidiaries with integrated risk assessments, pre/post system implementation assessments, IT security compliance audits, business continuity and disaster recovery plan reviews, IT service level reviews, data protection and privacy assessments. Mr. Kominars served as an adjunct professor at the University of Fairfax from 2002 to 2005 and was instrumental in developing and delivering graduate level instruction to adult learners in the Information Security domain. Prior to joining the University of Fairfax, he served as an adjunct professor at The George Washington University from 1995 to 2001 and provided graduate level instruction to the Executive MBA and MIS program in the area of systems analysis/engineering, database design, systems development w/CASE tools, and data communications. Mr. Kominars earned his MS in Information Systems from The George Washington University and his BA in Political Science from Virginia Polytechnic Institute.

***Certifications: CISM, CISA***

**David T. Lang** has over 30 years of experience in program management, training, counterintelligence, counterespionage, antiterrorism, security, and law enforcement. He currently serves as the Security Senior Manager at Dell and has previously managed major technical programs for industry, the Department of Defense, and several branches of the U.S. Intelligence Community. Mr. Lang served over 20 years in the United States Air Force retiring in 1998 as a Special Agent in Charge. He is a combat veteran and has served in numerous overseas locations in both military and civilian capacities. Mr. Lang has directly supported the U.S. Drug Enforcement Administration, the U.S. DoD Computer Forensics Laboratory, the National Reconnaissance Office, the DoD Counterintelligence Field Activity, and the U.S. Department of Homeland Security. He also served as a United Nations WMD inspector in Iraq in 2003. Mr. Lang is a senior member of the Institute of Electrical and Electronics Engineers (IEEE), a member of the Washington Field Chapter of InfraGard, the Northern Virginia Chapter of the Information Systems Security Association (ISSA), the Association of Former AFOSI Special Agents (AFOSISA), the Federal Law Enforcement Officers Association (FLEOA), and the Association for Intelligence Officers (AFIO).

***Certifications: CISSP, CISA, CISM, PMP, CPP, CAS, IAM***

**Thresa B. Lang, PhD** is a recognized leader in certification and accreditation for National Security Systems and a subject matter expert in Information Assurance Policy development and analysis. Currently, she serves as Corporate Security Strategist for Dell Global Security. Previously she was President of Lang Consultants Inc., an independent training and security consulting organization, where she handled computer and video forensics cases for private individuals and educational and private sector organizations. Her prior experience also includes positions as Vice President of Information Assurance and Technology for Special Aerospace Security Systems, Inc. and Director of Security and IT Training for Veridian. In addition, she served as an (ISC)<sup>2</sup> certified CISSP Review Seminar instructor and created a degree program in Digital Forensics for the George Washington University. Dr. Lang earned a PhD in Information Assurance Policy from the University of Fairfax; she holds an EdS from Nova Southeastern University, an MS in Management Information Systems from Bowie State University, and a BA in Education as well as a BA in French, both from the University of Wyoming.

***Certifications: CISSP, CISM, CISA***

**Lynn McNulty** spent most of his thirty-two year government career working in information security at a variety of agencies. He is now an independent consultant providing government affairs, business development, information security policy and program management consulting services to private and public sector clients. Mr. McNulty serves as the Director of Government Affairs for the International Information Systems Security Certification Consortium (ISC)<sup>2</sup> and represents the Information Systems Security Association (ISSA) on the Executive Board of the Information Technology Sector Coordinating Committee—one of the industry sector specific councils established by the Department of Homeland Security to implement the private/public cooperation model for protecting the nation’s critical infrastructure components. In March of 2005, he was appointed to the Information Systems Security and Privacy Advisory Board, established under the provisions of the Federal Information Security Management Act. This body advises the Director of the Office of Management and Budget, the Secretary of Commerce and appropriate Congressional committees of emerging issues that impact the security of federal information systems and the protection of personal information resident on these systems. Mr. McNulty served on the Board of Directors of (ISC)<sup>2</sup>, the governing body for the CISSP certification program from 1998 to 2005. He is the Co-Chair of the (ISC)<sup>2</sup> Government Advisory Board. He was awarded the “Industry Citation” at the 2007 meeting of the Colloquium for Information Systems Security Education in recognition of his contributions to the field of Information Security, and was recently inducted into the ISSA “Hall of Fame”. Mr. McNulty earned an MA in International Relations from San Jose State University, and an MS in Administration from the George Washington University. He also received a BA in Political Science from the University of California, Berkley.

***Certifications: CISSP***

**Bruce Morton** currently serves as Director, Business Development and Sr. Capture Manager at ManTech International. Previously he was Sr. Manager, Capture Excellence at Lockheed Martin Information Systems & Global Services. He has held prior positions as Principal Consultant at Lohfeld Consulting Group; Vice President, Capture Management at CACI; Director, Corporate Capture Management at Titan Corporation; Sr. Manager DoD Business Development at Lockheed Martin Information Technology; Director, Government Business Development at Lockheed Martin Global Telecommunications; Manager of Business Development at Lockheed Martin Management & Data Systems; Manager of Strategic Planning at Lockheed Martin and Rockwell International; and Spacecraft System Design Engineer at General Electric (GE Aerospace). He has authored and presented numerous conference presentations and proprietary papers with recent topics including Information Security, Information Warfare, Data Mining, and High Performance Computing. Mr. Morton has been the recipient of several awards, including Pioneer in Space Reconnaissance and Recovery from the National Reconnaissance Office. Mr. Morton holds an MS in Mechanical Engineering from University of Pennsylvania and a BS in Aeronautics and Astronautics from New York University.

**Ron Oklewicz** is the managing partner of iRoar Partners, where he is focused on helping small businesses reach their full potential by assisting them with strategic development, business development, and capital formation. Before starting iRoar, Mr. Oklewicz was the President of Inmedius, Inc., a Carnegie Mellon University spinout that provides web-centric, knowledge-based maintenance solutions for DoD. During his tenure with the company, it was recognized as one of the "Fastest Fifty Growing Technology Firms" in Western Pennsylvania by the Pittsburgh High Technology Council. Prior to Inmedius, Mr. Oklewicz was CEO, COO, and President of TelePad Corporation, a developer and manufacturer of advanced wireless mobile computers and software solutions. In addition to teaming with IBM on a worldwide ISO 9000 product development and manufacturing effort, he led the company's efforts in securing multiple rounds of financing, as well as NASDAQ initial and secondary public offerings. Previously, Mr. Oklewicz pioneered Apple Computer's effort in the federal marketplace as its first General Manager of Federal Operations, increasing annual revenues from \$3 million to \$154 million in four years. At Apple he was the executive-in-charge of securing and managing the Army's Automated Command and Control Systems (ACCS) procurement, the Joint Services World Wide Military Command and Control Contract (WWMCCS) and the World Wide Department of Defense Dependent Schools Contract (DODDS). Prior to Apple, he held senior sales and marketing positions at the Wollongong Group, an early developer of the Internet. He was the Vice President of Sales and Marketing and cofounder of Vidar Systems Corporation, a worldwide manufacturer of document scanners and document management software. At Dialcom, an online services company which pioneered electronic mail and the Congressional Correspondence System, he was responsible for sales and marketing activities that led to the company being acquired by ITT. Mr. Oklewicz has served on several Boards, including Sight Savers International, the American Family Society, the Armed Forces Communications and Electronics Association, as well as several corporate boards. He earned a BA from California University of Pennsylvania and completed the Strategic Marketing Management Program at the Stanford University Graduate School of Business.

**Mark D. Rasch, Esq.** currently serves as Director of CyberSecurity and Privacy Consulting at Computer Science Corporation. He has previously been a principal at secureITExperts.com, an information security and privacy consulting firm, and has worked with companies such as TJX on data breach and data breach disclosure investigations; developed data breach disclosure policies and procedures for members of the Direct Marketing Association; and developed information security and incident response policies and plans for Fortune 50 companies and major financial institutions. He worked with VISA and MasterCard to help develop the original PCI (Payment Card Industry) guidelines for securing payment systems. He was formerly a Managing Director for Technology at FTI Consulting, the Senior Vice President and Chief Security Counsel for Solutionary, Inc. and Vice President for Cyberlaw for Predictive Systems, Inc., where he provided computer security consulting and implementation services to the US government, intelligence and law enforcement agencies, and commercial enterprises. He is also a founding consultant to TruComply (now TruArx), specializing in PCI compliance solutions. For almost 10 years, Mr. Rasch lead the U.S. Department of Justice's efforts to investigate and prosecute computer and high-technology crimes, developing the DOJ initial guidelines on computer crime investigations, forensics and evidence gathering, and working with Congress to draft and revise computer crime and electronic evidence laws. He investigated and prosecuted the earliest computer crime cases including those of Kevin Poulsen, Kevin Mitnick and Robert T. Morris. Mr. Rasch has written and lectured extensively on computer crime, privacy, trademark, and trade secret issues on the Internet, and has been featured in *USA Today*, *The New York Times*, *NBC Nightly News*, *ABC's Nightline*, *PBS' Technopolitics*, *CNBC*, and *NPR* as an expert on computer law and policy. He authors a monthly column on law and technology on Symantec's *SecurityFocus* website, and is an occasional contributor to *Wired Magazine* and the *Intellectual Property Law Journal*. Mr. Rasch earned his JD from SUNY, Buffalo and his BA from SUNY, Albany.

**Larry Rosenfeld** is co-founder and CEO of Sage Communications, LLC. As a leading marketing communications professional for over 35 years, Mr. Rosenfeld lends his experience and expertise to developing branding strategies and tactical programs for Sage clients including major international, national and emerging technology companies and government agencies. Prior to Sage, he was the owner and president of one of the largest and most successful integrated marketing communications agencies for high-tech companies - Stackig Advertising and Public Relations (now TMP Worldwide). He was instrumental in the company's growth, developing the company into the largest full-service B2B and B2G agency in the Mid-Atlantic and one of the top 15 technology agencies in the nation. Mr. Rosenfeld has in-depth experience in all facets of marketing, branding, communications and public relations including market research, brand strategy, social media, advocacy, traditional and online advertising, media strategy, interactive and multimedia programs, direct marketing, trade shows, sales promotions, channel marketing, collateral literature, point-of-sale materials, merchandising and video production. A sampling of companies he has served include: AT&T Government Solutions, Juniper Networks Public Sector, Quest Software, Intelsat General, Comtech Mobile Datacom, Ciena, ManTech International, Northrop Grumman, Alcatel, Corvis, CACI, Newbridge Networks, Bosch Telecom, Cable and Wireless, SUPERCOMM, Hughes Network Systems, National Institute of Health, Department of Defense, General Services Administration, FreddieMac, FannieMae and many similar corporation and government agencies. In addition, Mr. Rosenfeld is chairman of the Government Marketing Forum, and serves on the steering committee for the Government Contractors Council. He earned a BS in Business/Journalism from the University of Maryland.

**Richard C. Schaeffer, Jr. (Dick)** served as the Director, Information Assurance at the National Security Agency (NSA). The Information Assurance Directorate (IAD) is the NSA mission element charged with providing products and services critical to protecting our Nation's critical information and information systems. IAD is also responsible for defining and implementing the Information Assurance Strategy to protect the Department of Defense's (DoD) Global Information Grid (GIG) and supporting ongoing military operations against terrorism by delivering solutions that allow the secure and dynamic sharing of information across security domains at multiple classification levels in today's net-centric environment. His career at NSA for over 30 years included positions as Director, National Security Operations Center, Information Assurance Deputy Director, Acting Associate Director for Research and NSA Deputy Chief of Staff. He also served as Director, Infrastructure and Information Assurance, Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) at the Pentagon. His numerous awards include the Presidential Rank Award and Secretary of Defense Medal for Meritorious Civilian Service Award. Mr. Schaeffer served in the United States Marine Corps. He earned a BSEE from the Catholic University of America.

**Joseph H. Schafer, PhD** has a proven record of interagency and industry leadership experience and achievement. He has led innovation as a defense industry executive with extensive experience as a government acquisition professional. He has served customers from the White House to the Intelligence Community and the Joint Staff to the Combatant Commands, Pentagon, and Federal Agencies. He has developed enterprise IT architecture and infrastructure; software as a service, virtualization, service oriented architecture, and cloud computing; enterprise logistics, personnel, and financial systems software development; and security engineering, IA, and cyber operations. Currently, he serves as Vice President for L-3 Communications- Strategic Technologies and Intelligent Solutions (STRATIS). He was promoted to Vice President and Program Manager in July 2008 after leading the team to win the White House IT infrastructure services for the Executive Office of the President of the United States. He serves as Vice President and Program Director for the U.S. Army Information Technology Agency IMCEN (HQDA DOIM) with department manager responsibility for Desktop Operations, Network Systems, Implementation, Service Desk, Information Assurance, Call Center, VTC, as well as Army Operations Center, Army Audit Agency, Defense Media Agency, and other customers. Previously he was Joint Program Manager for the CIO, US Transportation Command and prior to that he was the Product Manager for the Kuwait Iraq Command Control Communications & Computer (PM KICC); Program Executive Officer, Enterprise Information Systems where he formed a world-class team of 1,000 engineers, logisticians, contracting officers, technicians and specialists in the US, Kuwait and Iraq resulting in delivery of mobile and sustainable enterprise C4 systems. He was Senior Research Scientist and Assistant Professor at the United States Military Academy, Department of Electrical Engineering and Computer Science, West Point. While there he managed senior subject-matter experts as a founding leader of the annual IEEE Information Assurance Workshop and establishment of USMA as the first undergraduate institution certified by the NSA for academic excellence in information assurance. He also architected and implemented the Information Warfare Analysis & Research lab with the National Security Agency, directly resulting in the establishment of the annual NSA Cyber Defense Exercise competition. He was a “Federal 100 honoree” for uncommon dedication and unique vision across organizations to improve enterprise services. Dr. Schafer earned a Doctor and Master of Science in Computer Science from George Washington University, an MA in National Security and Strategic Studies at the US Naval War College and a BS in Electrical Engineering and Computer Science, US Military Academy, West Point.

***Certifications: PMP***

**Gary L. Tarbet, PhD** has over 15 years of information security experience and 30 years of IT operations management experience. Dr. Tarbet is a senior executive with System 1, Inc., where he provides Information Assurance and CIP support for multiple agencies including writing standards for NIST. Previously, he served with VeriSign as Practice Executive for information security, network engineering, managed services and enterprise management. He has held executive positions with Dotcom Platform, Big Sky Solutions, WinStar Telecommunications, National Electronics Warranty Companies, and SAIC. Dr. Tarbet earned his PhD in Information Assurance Policy from the University of Fairfax. In addition, he earned an Executive Masters in Information Systems from The George Washington University, as well as a dual MS in Oceanography and Meteorology from the Naval Postgraduate School, and a BS in Meteorology from the University of Utah.

***Certifications: CISA, CISSP-ISSMP, PMP***

## **BOARD OF DIRECTORS**

Joan Daly, Chair  
President, Daly Associates

Christopher V. Feudo, DSc  
Vice President, Edgewater Federal Solutions; CEO, Secureant

Roger C. Gurner  
Executive Vice President, CoVant

Hugh Kominars  
Vice President, ControlCase

David Oxenhandler  
President, University of Fairfax

William J. Solomon  
President, The Serengeti Group

## ACADEMIC CALENDAR



### University of Fairfax ACADEMIC CALENDAR Calendar Year 2012

#### **Spring Term 2012**

Dec 16 2011	Registration period begins
Dec 30 2011	Registration period ends
Jan 02 2012	New Year's Day Holiday (Offices Closed)
Jan 06 2012	Online course preview begins
Jan 08 2012	Course session begins; instruction begins
Jan 11 2012	Course Add deadline
Jan 14 2012	SyncSession 1; Course Drop deadline
Jan 16 2012	MLK Holiday (Offices Closed)
Jan 28 2012	SyncSession 2
Feb 11 2012	SyncSession 3
Feb 23 2012	Deadline to request Incomplete
Feb 25 2012	SyncSession 4; Course Withdrawal deadline
Mar 03 2012	Course session ends
Mar 31 2012	Deadline for Incomplete assignments

#### **Course Session I**

#### **Spring Term 2012**

Feb 10 2012	Registration period begins
Feb 24 2012	Registration period ends
Mar 02 2012	Online course preview begins
Mar 04 2012	Course session begins; instruction begins
Mar 07 2012	Course Add deadline
Mar 10 2012	SyncSession 1; Course Drop deadline
Mar 24 2012	SyncSession 2
Apr 07 2012	SyncSession 3
Apr 19 2012	Deadline to request Incomplete
Apr 21 2012	SyncSession 4; Course Withdrawal deadline
Apr 28 2012	Course session ends
May 26 2012	Deadline for Incomplete assignments

#### **Course Session II**

#### **Apr 29 2012 – May 05 2012**

#### **Term Break**

#### **May 19 2012**

#### **Commencement Ceremony**

#### **Summer Term 2012**

Apr 13 2012	Registration period begins
Apr 27 2012	Registration period ends
May 04 2012	Online course preview begins
May 06 2012	Course session begins; instruction begins
May 09 2012	Course Add deadline
May 12 2012	SyncSession 1; Course Drop deadline
May 19 2012	Commencement Ceremony
May 26 2012	SyncSession 2
May 28 2012	Memorial Day (Offices Closed)
Jun 09 2012	SyncSession 3
Jun 21 2012	Deadline to request Incomplete
Jun 23 2012	SyncSession 4; Course Withdrawal deadline
Jun 30 2012	Course session ends
Jul 28 2012	Deadline for Incomplete assignments

#### **Course Session I**

**Summer Term 2012**

Jun 08 2012	Registration period begins
Jun 22 2012	Registration period ends
Jun 29 2012	Online course preview begins
Jul 01 2012	Course session begins; instruction begins
Jul 04 2012	Independence Day Holiday (Offices Closed)
Jul 05 2012	Course Add deadline
Jul 07 2012	SyncSession 1; Course Drop deadline
Jul 21 2012	SyncSession 2
Aug 04 2012	SyncSession 3
Aug 16 2012	Deadline to request Incomplete
Aug 18 2012	SyncSession 4; Course Withdrawal deadline
Aug 25 2012	Course session ends
Sep 22 2012	Deadline for Incomplete assignments

**Course Session II**

**Aug 26 2012 – Sep 01 2012**

**Term Break**

**Fall Term 2012**

Aug 10 2012	Registration period begins
Aug 24 2012	Registration period ends
Aug 31 2012	Online course preview begins
Sep 02 2012	Course session begins; instruction begins
Sep 03 2012	Labor Day Holiday (Offices Closed)
Sep 05 2012	Course Add deadline
Sep 08 2012	SyncSession 1; Course Drop deadline
Sep 22 2012	SyncSession 2
Oct 06 2012	SyncSession 3
Oct 18 2012	Deadline to request Incomplete
Oct 20 2012	SyncSession 4; Course Withdrawal deadline
Oct 27 2012	Course session ends
Nov 24 2012	Deadline for Incomplete assignments

**Course Session I**

**Fall Term 2012**

Oct 05 2012	Registration period begins
Oct 19 2012	Registration period ends
Oct 26 2012	Online course preview begins
Oct 28 2012	Course session begins; instruction begins
Oct 31 2012	Course Add deadline
Nov 03 2012	SyncSession 1; Course Drop deadline
Nov 17 2012	SyncSession 2
Nov 22-23 2012	Thanksgiving Holiday (Offices Closed)
Dec 01 2012	SyncSession 3
Dec 13 2012	Deadline to request Incomplete
Dec 15 2012	SyncSession 4; Course Withdrawal deadline
Dec 22 2012	Course session ends
Dec 25 2012	Christmas Holiday (Offices Closed)
Jan 02 2013	New Year's Day Holiday (Offices Closed)
Jan 21 2013	Deadline for Incomplete assignments

**Course Session II**

**Dec 23 2012 – Jan 05 2013**

**Session Break**