Master of Science in Information Security and Assurance (formerly Master of Science in Information Assurance)

Program Overview

Program Director: Chrisan Herrod

The Master of Science in Information Security and Assurance (formerly Master of Science in Information Assurance) program's mission is to deliver a state-of-the-art, high-quality, and convenient education to busy professionals committed to furthering their careers in information security and assurance. In particular, the Master of Science in Information Security and Assurance program will appeal to chief information, technology, and information security officers of business and governmental organizations. Additionally, it is designed for security administrators, network administrators, information technology specialists, professionals in the information technology field, and military personnel. Master of Science in Information Security and Assurance graduates are leaders and innovators in information security and assurance, bringing sound interdisciplinary perspectives to the field.

The program balances academic rigor with convenience. This combination maintains and respects Norwich University's long educational heritage while it meets the needs of today's working students. The program hires instructors of high professional stature and demands highly personal and extraordinary academic interactions with students.

The program's information security and assurance curriculum includes exploration of the current state of the information security and assurance marketplace. White papers, Web sites, discussion groups, conference proceedings, professional association meetings – all provide opportunities to learn about which products and services are being discussed and used by practitioners of information security and assurance.

The case study is a required part of the Master of Science in Information Security and Assurance program and each student is required to demonstrate access to an organization which will serve as their case study during the program. Throughout the program, students read about and discuss the topics at hand; as they study various aspects of information security and assurance, students must analyze the situation at their workplace or case study site every week with respect to the week's topics. Students use their research findings to prepare a report with recommendations for improvement of specific areas of information security and assurance to be submitted in the last week of each seminar to the program's instructors and to the appropriate people within the case-study organization.

Curriculum Map

Semester 1	Credits	Semester 2	Credits	Semester 3	Credits
GI 512 Foundations and Historical Underpinnings of Information Assurance	6	GI 532 Human Factors and Managing Risk	6	Select one concentration course	6
GI 522 Information Assurance Technology	6	GI 542 Information Assurance Management and Analytics	6	Select one concentration course	6
				GI 595 Residency[1]	0
	12		**12**		**12**

Total Credits: 36

[1] Students are required to attend a one-week, on campus Residency Conference the June following or concurrent with their final course.

Curriculum Requirements

Four of the six seminars in the 36 credit hour program are core requirements and two courses comprise an elective concentration. All courses are focused on providing an opportunity for students to acquire and exercise the knowledge and skill expected of top-level managers of information security and assurance in today's demanding security environment.

Required Core Courses (24 credits)

GI 512	Foundations and Historical Underpinnings of Information Assurance	6
GI 522	Information Assurance Technology	6
GI 532	Human Factors and Managing Risk	6
GI 542	Information Assurance Management and Analytics	6
Culminating Academic Requirement		
GI 595	Residency	0
Total Credits		24

Concentrations (12 credits)

One of the following two-seminar, 12-credit concentrations is required to complete the 36 credit hour program: Computer Forensic Investigation/ Incident Response Team Management; or Private Sector Business Continuity Management.

Computer Forensic Investigation/Incident Response Team Management		
GI 551	Computer Forensic Investigations	6

GI 554	Computer Security Incident Response Team Management	6
Total Credits		12

Private Sector Business Continuity Management

BC 510	Foundations of Business Continuity Management	6
BC 520	Principles of Incident Management and Emergency Response	6
Total Credits		12

One-Week Residency

During the final phase of the Master of Science in Information Security and Assurance program students are required to attend a one-week residency on the Norwich University campus. During this residency, students may attend professional presentations, participate in roundtable discussions with faculty, and present papers. The one-week residency is a degree requirement.

Faculty Member	Institution at which highest degree was earned
Martin J. Devine, MA, CISSP, CISM, CBCP	Naval War College
Cris Ewell, PhD, CISSP, CISM	Nova Southeastern University
Robert Guess, MSIA, CISSP, NSA-IAM, -IEM	Norwich University
Dawn Hendricks, MSSE, CISSP	Johns Hopkins University
Thomas Hendricks, MESCS, CISSP	Loyola College (MD)
Rebecca Herold, MA, CISSP, CISM, CISA, FLMI	University of Northern Iowa, Cedar Falls
Donald Holden, MBA, CISSP-ISSMP	University of Pennsylvania
John Mason, MBA, CISA, CISM, CFE, CFSSP, CFS	University of Phoenix
Michael Miora, MA, CISSP-ISSMP, FBCI	University of California, Berkley
Dennis Opacki, MSIA, CISSP	Norwich University
Ric Steinberger, MSME, CISSP	Catholic University
George Silowash, MSIA, CISSP	Norwich University
Peter R. Stephenson, PhD, CISSP, CISM, FICAF	Oxford Brookes University

Business Continuity Courses

BC 510. Foundations of Business Continuity Management. 6 Credits.
This seminar introduces students to the field of Business Continuity Management with an emphasis on the steps needed to develop a business continuity plan and risk management program. Students will learn about the functions and goals of a business continuity manager, and will experience first-hand the challenges of developing a continuity plan. Weekly sessions target the major steps in plan development such as project initiation, risk and business impact analysis, risk mitigation and control strategy development and implementation, response strategies, plan testing, as well as the organizational structure needed to sustain a continuity program over time.

BC 511. Continuity of Government Operations. 6 Credits.
This course teaches all of the elements needed to develop a Continuity of Operations plan for a governmental agency. The topics include organizational analysis, risk and threat analysis, mitigation.

BC 520. Principles of Incident Management and Emergency Response. 6 Credits.
This seminar teaches how to develop a plan for responding to a business disruption. Topics will include response procedures, notification, communication, and event management. Students will also learn how to manage public perceptions, and work with outside agencies and public sector emergency responders during and after an incident.

BC 521. Public Sector Incident Management and Emergency Response. 6 Credits.
This course teaches how to respond to incidents that effect governmental agencies. The topics include developing a response plan, emergency operations centers, emergency communication, and working with the first responder community. Students will also learn how to develop off-site backups and work areas, and how to get people and equipment in place for continuing operations during an emergency.

BC 595. Residency. 0 Credits.

Graduate Info. Assurance Courses

GI 512. Foundations and Historical Underpinnings of Information Assurance. 6 Credits.
This seminar explores the historical foundations of information assurance from the early days of mainframes to the foundations of today's sophisticated networks and distributed computing systems. It examines the earliest thinking about data structures and domains, interoperability between different computing platforms and mechanisms for data transfer and proceeds to the emergence of encryption as a defense against early forms of computer crime. This seminar looks at privacy, policies, and security standards and regulatory requirements. Finally, the seminar addresses the underlying models that define information assurance and takes a first look at IA architecture.

GI 522. Information Assurance Technology. 6 Credits.
This seminar focuses on the use of technological defenses against threats and exploitations of vulnerabilities in information systems. Topics include physical security measures, access controls, security elements of operating systems, network security measures, anti-malware tools, anti-spam measures, anti-piracy systems, software development methods supporting security, and security certifications for software products.

GI 532. Human Factors and Managing Risk. 6 Credits.
This seminar focuses on the ways that business objectives, user attitudes and user activities significantly influence both the development of an information assurance program and its successful implementation. The first week focuses on Operations Security and why it is the foundation for an IA program and the key to the program's effectiveness. The following five weeks explore security awareness as a component of organizational culture: crafting the information assurance message; understanding ethical decision- making as a factor in security; understanding social psychology and how behaviors will influence the effectiveness of security activities; using employment practices and policies to support information security; and creating Acceptable Use and e-mail policies. The final four weeks examine different elements of Risk Management from basic principles through application. The NIST Special Publication 800-30 provides a solid foundation for the risk management issues. Two popular risk assessment processes, and several other processes that help identify risk will be discussed.

GI 542. Information Assurance Management and Analytics. 6 Credits.
This seminar is arranged in four general areas beginning with examining and exploring the strategic and gradually narrowing down to the tactical level: Compliance -> Management, Leadership, & Policy Development -> Relationships & Adding Value -> Project Management. The curriculum explores the aspects, methods, and alternatives in information assurance management and compares/utilizes them with respect to non-IT-related management approaches and styles. Additionally, it explores alternatives in building support and consensus for projects and activities and focuses heavily on adding value to the organization. Developing an information assurance marketing plan is examined and is used to help identify techniques of improving the information assurance awareness. Analytics are explored both in terms of metrics and measuring business impact and problem solving and project management techniques and alternatives are included.

GI 551. Computer Forensic Investigations. 6 Credits.
This course focuses on the spectrum of tools and techniques used to investigate digital incidents whether in a civil or criminal environment. Information assurance professionals are expected to have a broad understanding of digital incidents, their management, investigation and analysis. This seminar provides that broad understanding and places it in the context of other information assurance domains. These discussions of digital investigation and forensics cover topics from both the technical and management perspectives. This coverage aids the information assurance professional's understanding and application of domain-specific knowledge.

GI 554. Computer Security Incident Response Team Management. 6 Credits.
Students will analyze and apply the key points in creating and managing a computer security incident response team (CSIRT), also sometimes known as a computer incident response team (CIRT) or a computer emergency response team (CERT). Major topics include establishing CSIRTs; responding to computer emergencies; securing the CSIRT; managing the CSIRT with respect to professionalism, setting priorities for triage, and protecting personnel against burnout; and learning from emergencies using the incident postmortem and by establishing continuous process improvement within the organization. Students will use their case study to apply their knowledge to real-world situations and will prepare recommendations for establishment of a new CSIRT or improvement of their existing CSIRT.

GI 562. Penetration Testing I. 3 Credits.

GI 563. Penetration Testing II. 3 Credits.

GI 595. Residency. 0 Credits.