Graduate Info. Assurance (GI)

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.