Info Security/Assurance (ISA) Courses

ISA5005 Network Fundamentals
This course is a foundational graduate-level course in computer networks. The course offers a comprehensive review of the application, transport, network and link layers of the OSI protocol stack. Advanced topics, including network management, traffic engineering and router configuration, are also addressed. Network protocols are studied in detail with an emphasis on learning to read RFCs within the context of the structure, FSM, configuration protocol learning paradigm.
Offered at Online, Providence
3 Semester Credits

ISA5020 Foundations of Information Security Management
This courses provides a conceptual overview of information security management and information assurance (IA). Topics covered at an introductory level include information security and information assurance principles, information technology security issues, and security technologies and processes. Governance issues include policy, law, ethics and standards, as well as organizational models and communications. Risk management issues include risk assessment, threats, vulnerabilities and security life-cycle management.
Offered at Online, Providence
3 Semester Credits

ISA5030 Legal and Ethical Principles in IT
This course provides an in-depth working knowledge of the ethics and laws pertaining to information systems security. Topics include the ethics of privacy, confidentiality, authenticity, medical information, copyright, intellectual freedom, censorship, social networking and cyber-bullying. Issues related to the creation, implementation, enforcement and assessment of institutional codes of ethics are discussed.
Offered at Providence
3 Semester Credits

ISA5040 Network Security and Cryptography
This course details the issues faced by security managers in addressing network security threats, technical discourse regarding known threats, potential countermeasures to these threats, and the need for the aggressive application of cryptographic methods to guarantee the security of information. Students are immersed in the details of cryptography and explore both symmetrical and asymmetrical methods. Students delve into both the technological and mathematical elements of cryptography.
Prerequisite(s): ISA5005 or Department Chair Approval.
Offered at Providence
3 Semester Credits

ISA5050 Digital/Computer Forensics and Investigation
This course studies cyber-attack prevention, planning, detection, response and investigation. Course goals include counteracting cybercrimes, and identifying and making the responsible persons/groups accountable. Topics covered in this course include fundamentals of digital forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anti-forensics techniques, anonymity and pseudonymity, cyber law, computer security policies and guidelines, court report writing and presentation, and case studies.
Prerequisite(s): ISA5040.
Offered at Providence
3 Semester Credits

ISA5085 Principles of Programming
This course teaches students without a background in computer science or software engineering the concepts necessary to complete the graduate program in Information Security/Assurance. This course is designed to deliver an understanding of core algorithmic concepts (e.g., control structures, assignment, decision structures, mathematical/Boolean operations, etc.), an introduction to structured and object-oriented computer programming languages, compilers, interpreters and virtual machine environments. Students design algorithms to solve problems and learn how to translate these algorithms into working computer programs using appropriate languages and runtime environments.
Offered at Providence
3 Semester Credits

ISA6010 Software Security Testing
This course teaches the fundamentals of software testing from the viewpoint of security. An in-depth discussion on various security testing methods and tools vulnerabilities is provided with demos of concepts during the class. Students learn how to perform penetration testing in a practical way using well-established tools such as Kali Linux. This course covers different types of systems including Web-based systems and some internals of OS kernel software testing and exploitation. Students also learn software design patterns to built-in security during the architectural phase of the life-cycle.
Prerequisite(s): ISA5085, completion of 15 credits from core courses.
Offered at Providence
3 Semester Credits

ISA6020 Securing Virtualized and Cloud Infrastructures
This course is designed to give students a solid technical understanding of virtualization, cloud computing, storage networks and the vulnerabilities known to exist in these environments. Students gain an understanding of the planning of these environments, the countermeasures to threats that exist and the management of information in the cloud. Topics include the interconnection of the virtualized environment with the underlying network transport and network storage technology.
Prerequisite(s): ISA5040.
Offered at Providence
3 Semester Credits

ISA6030 Hacking Countermeasures and Techniques
This course focuses on the study of well-known hacker tactics, attack typing and categorization, profiles of hacker strategies, and a detailed review of countermeasures. Students examine both active and passive attacks, vulnerabilities of operating systems and the software vulnerabilities of popular systems with an eye toward effectively thwarting hacker threats.
Prerequisite(s): ISA5085, completion of 15 credits from core courses,
Corequisite: ISA6040.
Offered at Providence
3 Semester Credits

ISA6040 Advanced Network Intrusion Detection and Analysis
This course covers principles and techniques of intrusion detection such as network traffic analysis, packet analysis, application protocol layer for common protocols, and log analysis. The use of intrusion detection tools and services is evaluated, as intrusion detection systems are now integral parts of the technology management fabric with the capability to stop threats in progress and capture/quarantine evidence.
Prerequisite(s): ISA5085, completion of 15 credits from core courses,
Corequisite: ISA6030.
Offered at Providence
3 Semester Credits

ISA6050 Business Continuity Planning
This course focuses on the need for and ability to conduct business continuity planning. Emphasis is on planning for the inevitable system failure, network fault or security breach in the current technological environment, given industry's heavy reliance on technology.
Prerequisite(s): ISA5020, completion of foundation courses.
Offered at Online, Providence
3 Semester Credits

ISA6060 Risk Management and Incident Response
This course is directed toward students interested in understanding how large-scale complex risk can be quantified, managed and architected. Students learn to identify the business and technical issues, regulatory requirements and techniques to measure and report risk across a major organization. Students explore techniques used to mitigate, minimize and transfer risk. This course also provides a foundation in disaster recovery principles, addressing concepts such as incident disaster recovery planning, developing policies and procedures, roles and relationships of various members of an organization, "swim lane" diagramming, implementation of the plan, testing and rehearsal of the plan, planning disaster recovery resources, and linking risk management incident response to large-scale disaster recovery implementations planning; developing policies and procedures; roles and relationships of various members of an organization; “swim lane” diagraming, implementation of the plan; testing and rehearsal of the plan; planning disaster recovery resources, linking risk management incident response to large scale disaster recovery implementations.
Prerequisite(s): ISA5020, completion of foundation courses.
Offered at Online, Providence
3 Semester Credits

ISA6070 Cyber Science and IT Business Operations
This course focuses on IT auditing processes, cyber threats and their effect on common infrastructures, the properties and applications of specific loss count and loss severity distributions, actuarial modeling, and forensic accounting techniques. Topics include the planning of security provisions, countermeasures and deployment, as well as understanding the impact of attacks (evidence gathering and investigation), which depend on a combination of technology and business acumen. Certain estimation methods like percentile matching, maximum likelihood estimation, Bayesian estimation and credibility theory are also introduced.
Prerequisite(s): ISA5020, completion of foundation courses.
Offered at Online, Providence
3 Semester Credits

ISA6090 Information Security & Assurance Capstone Research Project
This capstone course integrates previous coursework and practical experience with a focus on authentic demonstration of competencies outlined by the program. Students synthesize prior learning to design or develop a capstone as a culmination of their studies. The course is structured to support student success in fulfilling program requirements and developing a well-thought-out, comprehensive capstone project. Problem domains may be suggested by external sponsors, the instructor or student teams. The project itself can be research-oriented, have a design focus, center on evaluation and testing, or be tailored to an individual or team's interests. It should, however, touch on either the technical or business elements of information security, or a combination of both. Student teams or individuals are expected to document their projects in a weekly, online process journal. Key deliverables for the course, regardless of the project definition, include planning documents, execution plan, final project deliverable and presentation. Problem domains may be suggested by external sponsors, the instructor, or student teams. The project itself can be research-oriented, have a design focus, center on evaluation and testing, or be tailored to an individual or team’s interests. It should, however, touch on either the technical elements, the business elements, or the combine technical & business elements of information security. This delivery model requires good communication about the process, as well as, the results of a project, since that is the main focus of the learning in the capstone experience. As such, student teams or individuals are expected to document their projects in a weekly, online process journal. Key deliverables for the course, regardless of the project definition, include planning documents, execution plan, final project deliverable and presentation.
Prerequisite(s): Completion of 9 credits from selected Technical or Business focus area and all core courses.
Offered at Providence
3 Semester Credits