Information Assurance Management (IAM)

IAM 409 Management of Information Assurance (3 Sem. Hrs.)

Prerequisite: AC/MG 302 or equivalent

This course focuses on the managerial aspects of information security and assurance. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. The course includes up-to-date information on changes in the field, such as national and international laws and international standards like the ISO 27000 series.

IAM 410 Information Assurance Administration and Operations Management (3 Sem. Hrs.)

Prerequisite: AC/MG 302 or equivalent

This course presents a focus on a managerial view of data and system security. Topics include security policy development, risk management, threat assessment, and business continuity planning. The aim is to examine the implications and challenges of operational security in global organizations. This course provides students with an understanding of the legal, social, and ethical issues related to security management from the management perspective. The course also covers the importance that management and administrators place on information security, as it pertains to overall business risk, social issues such as individual privacy, and the role of public policy.

IAM 411 Information Assurance Strategic Management (3 Sem. Hrs.)

Prerequisite: AC/MG 302 or equivalent

A survey of various means of establishing and maintaining a practical cyber and information security program to protect key organizational assets. The aim is to develop an information security program that is aligned with organizational strategy and to evaluate and recommend information and security technologies to support the information security program. Discussion covers the integration of confidentiality, integrity, and availability into an organization's security program through the use of physical and logical security controls. Topics include data protection, telecommunications systems, applications, and emerging technologies. Threats and vulnerabilities are assessed to determine the level of risk.

IAM 412 Management of Business Contingency and Resilience Planning (3 Sem. Hrs.)

This course prepares students to plan and execute industry best practices related to managing organization-wide business contingency and resilience programs and to prepare an organization for implementing comprehensive business continuity, incident handling, and disaster recovery plans.

IAM 413 Information Assurance Systems and Product Acquisition (3 Sem. Hrs.)

Acquisition strategy can be seen as a high level framework that guides program execution across the entire program life cycle. Acquisition strategies typically look for innovative ways to reduce costs. One such way is to consider the security implications of a particular process or automated resource prior to introducing it into the organization. This course explores the security controls established by the National Institute of Standards and Technology (NIST) and evaluates methods for integrating the controls into the acquisition process.

IAM 414 Information Assurance Governance (CAPSTONE) (3 Sem. Hrs.)

This course gives students a detailed understanding of the broad requirements for effective information security governance, the elements and actions required to develop an information security strategy and a plan of action to implement it.