



## GRADUATE CERTIFICATE IN **Information Assurance and Security**

### Certificate Description

**This certificate provides experienced professionals who possess a bachelor's degree the ability to obtain specialization in the field of Information Assurance and Security to grow professionally.**

**Principles of Information Security—ITAS 661**—This course covers information security technologies as applied to operating systems, database management systems, and computer networks. The three major goals of information security, confidentiality, integrity, and availability, are introduced. Threats, vulnerability, exposure, risks, identity management, incidents response, the state machine model, and disaster recovery are also covered.

**Outcomes:**

- Discuss the framework and concepts of information security and privacy
- Explain the issues related to prevention, detection, and response
- Justify the preferred approach for handling an incident
- Explain cryptography, business continuity, and disaster recovery from a business perspective
- Make decisions related to company data security and explain the impact of those decisions on an organization
- Compare internal and external information security solutions for a given situation

**Applied Cryptography and Network Security—ITAS 663**—In this course, students learn to apply secure protocols over networked systems using cryptography. Symmetric and asymmetric encryption is covered. Other topics that are also covered include one way function, hash, cryptography arithmetic, public key infrastructure, Digital Signature Algorithm, and Internet security issues.

**Outcomes:**

- Identify unsound security practices in software systems.
- Discuss commonly used authentication protocols used in current Internet technology.
- Explain common vulnerabilities in cryptographic protocols and how they can be avoided.
- Describe the use of industry-current algorithms in Internet security.



## GRADUATE CERTIFICATE IN **Information Assurance and Security**

**Legal Issues in Information Security and Incident Responses—ITAS 665**—In this course, students explore current issues in network security and apply security concepts. The class focuses on technical topics as well as privacy and policy issues. Computer crimes, evidence presentation, chain of custody, and introduction to the United States criminal justice system are also covered.

**Outcomes:**

- Explain different crimes that are committed on a computer or with a computer and explain the general motives of cyber criminals.
- Describe various viruses and hostile codes that are used to compromise computer systems.
- Discuss how to secure a security crime area and be able create incident response procedures and complete a chain of custody form.
- Describe different areas in the Windows and UNIX computers that data can be hidden from forensic investigators.
- Analyze forensic tools and demonstrate a mastery of the functions and usage of at least three forensic tools.

**IT Auditing and Security Risk Management—ITAS 669**—The course covers information systems control, application audit, security threats, security risk types, computer attacks, countermeasures, and risk management. Risk assessment methodologies, certification, accreditation, information systems auditing, and metrics for measuring an organization's information security program are also covered in this course.

**Outcomes:**

- Explain the functions of an information systems auditor and the types of audits that can be performed on information systems
- Describe and outline the steps involved in information systems risks assessment
- Compare the goals of information systems audit and security risk assessment
- Create information security audit or risk assessment report
- Create security certification and accreditation package