Graduate Certificate - Information Assurance

The graduate certificate in Information Assurance teaches the theory and technical skills needed to detect threats and to secure vital, sensitive information assets across enterprise networks for organizations and government agencies. Achieving credentials in the information assurance (IA) field helps prove your knowledge of: network security solutions; continuous monitoring, activity analysis, threat detection, warnings, and attacks; cryptography; security awareness training and support; and infrastructure security engineering. This certificate program is intended for graduate students who seek to heighten their knowledge of information assurance without committing to an academic degree program.

This program has specific admission requirements.

Certificate Objectives

Upon successful completion of this certificate, the student will be able to:

- Analyze the components of an information assurance and certification plan.
- Assess security governance objectives and risk management objectives.
- Examine the phases, processes, standards, the levels, and the process areas of the INFOSEC Assessment Capability Maturity Model (IA-CMM).
- Appraise and conduct a complete threat, vulnerability, impact, and risk assessment; and synthesize risk mitigation strategies based on the analysis of this data.
- Evaluate the processes and deliverables of the INFOSEC assessment methodology (IAM).
- Design relevant information security management metrics by analyzing incident management and response data.

Programmatic Admission Requirements

For this program, you must provide an official transcript of your previously completed bachelor's or master's degree and have ONE of the following:

- Associate or bachelor's degree in information technology or a related field (ex: computer science, information systems, database development, etc.)
- 2 years of work experience in the specific sub-field for this degree
- Completion of one of our undergraduate IT certificates
- Completion of 6 credits in IT-related courses
- Completion of an IT-related minor or concentration during your undergraduate program
- Certifications in at least one of the below, should be active and earned since 2010:

  1. CompTIA Security+
  2. CompTIA Network+
  3. CompTIA A+
  4. CompTIA Project+
  5. CISSP certification
  6. SSCP
  7. EC-Council Ethical Hacking
  8. Cisco CCNA Security
  9. Project Management Professional certification from the Project Management Institute

Notes:

- If the IT-specific requirements are not noted in the official bachelor's or master's transcript, you must provide official copies of your undergraduate transcripts that show the appropriate coursework.
- The verification of the 2 years' work experience needs to be sent to the university via formal resume/CV.
- Preadmission courses completed at the undergraduate level must be graded C or better; B or better at the graduate level.

Please visit our AMU (https://www.amu.apus.edu/admissions/graduate-requirements.html) or APU (https://www.apu.apus.edu/admissions/graduate-requirements.html) graduate admission page for more information on institutional admission requirements.

Need help?

If you have questions regarding a program's admission requirements, please contact an admissions representative at 877-755-2787 or info@apus.edu.

Certificate Requirements (18 semester hours)

Code	Title	Semester Hours
ISSC640	Computer Networks and Data Systems	3
ISSC641	Telecommunications and Network Security	3
ISSC660	Information Assurance	3
ISSC661	Information Assurance: Assessment and Evaluation	3

ISSC662	Information Assurance: Capability Maturity and Appraisals	3
ISSC680	Information Security Management	3
Total Semester Hours		18