Master of Science in Information Technology

The Master of Science in Information Technology focuses on the development and implementation of information systems and includes topics such as database systems, object-oriented analysis and design, IS architectures, IT project management, security, and computer forensics. In this graduate program, you will study the theory, principles, best practices, tools, and technologies associated with the IT marketplace. You'll also be taught the analytic, problem-solving, and research skills required to solve real world business problems.

This program has specific admission requirements.

Degree Program Objectives

In addition to the institutional and degree level learning objectives, graduates of this program are expected to achieve these learning outcomes:

- Apply key management theory, principles, best practices, tools, and technologies associated with information systems.
- Analyze selected research methods and tools.
- Utilize graduate level critical thinking, reasoning, and writing to defend the logic and the conclusions in scholarly research.
- Plan the processes, phases, domains, and measures for effectively managing complex information technology projects.
- Design a normalized and optimized enterprise database system.
- Produce a plan that addresses the principles and challenges in incorporating emerging network architectures, technologies, and protocols into information technology systems.
- Develop legal, social, ethical, and technical solutions for securing information systems.
- Assess the vulnerabilities of information systems with respect to security and the methodologies to mitigate this risk.
- Perform in-depth research and critical analysis on thesis subject or creative project.

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:
  a. CompTIA Security+® (2010 to present recommended)
  b. CompTIA Network+® (2010 to present recommended)
  c. CompTIA A+® (2010 to present recommended)
  d. CompTIA Project+® (2010 to present recommended)
  e. CISSP® certification (valid up until the expiration date)
  f. SSCP®
  g. EC-Council Ethical Hacking
  h. Cisco CCNA® Security
  i. A valid and current Project Management Professional certification from the Project Management Institute

CompTIA Security+®, CompTIA Network+®, CompTIA A+®, and CompTIA Project+® are all registered trademarks of the Computer Technology Industry Association, Inc.

CISSP® and SSCP® are registered trademarks of International Information Systems Security Certification Consortium, Inc

CCNA® is a registered trademark of Cisco Technology, Inc.

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.

Degree at a Glance

Code	Title	Semester Hours
Core Requirements		18
Select one of the following concentrations:		15
Digital Forensics (p. 2)		
Information Assurance and Security (p. 2)		
IT Project Management (p. 3)		
Final Program Requirements		3
Total Semester Hours		36

Degree Program Requirements

Core Requirements (18 semester hours)

Code	Title	Semester Hours
INFO531	Management Information Systems [1]	3
ITCC500	Research Methods in Information Systems and Technology	3
INFO620	Enterprise Database Systems	3
ISSC640	Computer Networks and Data Systems	3
ISSC680	Information Security Management	3
ITMG624	Information Technology Project Management	3
Total Semester Hours		18

[1] Required as the first course in this program.

Students must choose a concentration for this degree program and may select from the Concentration in Digital Forensics, Concentration in Information Assurance and Security, or Concentration in IT Project Management.

Concentration in Digital Forensics (15 semester hours)

The societal impact of cybercrime has become commonplace; it is broadcast on the evening news and is a favorite playing field for television shows and moviemakers. Technology is a boon to society, but, in malicious hands, it becomes a valuable instrument in a dark and sinister underworld; and, unfortunately, cyber legislation and forensics have been lagging way behind when it comes to cybercrime. The process of forensics investigation can destroy the very evidence it is seeking to assimilate. The window of opportunity for collecting evidence can be a few seconds or minutes depending on the sophistication of the perpetrator. This concentration pertains to the study of various forensics models to identify, preserve, collect, examine, analyze, prepare, and present evidence for prosecuting cybercrime.

Objectives

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

- Evaluate data security, integrity, exposure from multifunctional devices, tracking techniques, and forensics models for analysis and examine the inherent challenges in the processes for seizing electronic evidence.
- Evaluate the principles, practices, and inherent challenges of the e-discovery process and assess the tools, techniques, and procedures to legally seize and forensically evaluate digital crime scenes.
- Analyze concealment and cloaking techniques and technologies such as cryptography, steganography, and data hiding and investigate corresponding legislation and mitigation techniques.
- Assess and mitigate potential exposures and the risks of the chain of custody and examine the methodologies to mitigate the potentially narrow window of opportunity for collecting digital evidence. Investigate models to examine the financial and societal impact of technology-related crime.
- Appraise the legal and regulatory compliance requirements in investigating and prosecuting technology-related crimes.

Concentration Requirements (15 semester hours)

Code	Title	Semester Hours
ISSC621	Computer Forensics	3
ISSC630	Advanced Cybercrime Analysis	3
ISSC631	Cyber Ethics: Privacy and Intellectual Property	3
ISSC650	Advanced Digital Forensics	3
ISSC651	Advanced eDiscovery	3
Total Semester Hours		15

Concentration in Information Assurance and Security (15 semester hours)

The primary challenge for ecommerce is assuring the security and integrity of information systems. We are bombarded daily by news of viruses, worms, malware, breaches, infiltrations, denial-of-service attacks, and the like. The ability of an organization to secure and assure its information technology assets is essential to conducting global commerce and to establishing a robust economy; this is a particular challenge given the rapidly changing face and assets of the virtual intruder. The ability to compromise an organization's information assets is a direct threat to their competitive advantage; and the ability

to protect the information assets of an organization is essential to maintaining clientele, trust, revenue streams, credibility, and the survival of the organization. This concentration focuses on securing the information technology assets of an organization. Areas include network security, telecommunications security, computer forensics, legal and ethical issues, cybercrime, computer forensics, information assurance, security risk mitigation, information systems audit and certification, intrusion detection, and incident handling.

Objectives

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

- Profile the emerging security threats and trends, and analyze the information systems vulnerabilities that they exploit.
- Assess the methods and techniques for recognizing and profiling attack patterns.
- Categorize and analyze the different types of cryptography, encryption keys, malicious software, and types of attacks.
- Analyze the methodologies for investigating computer-related crime and for incident handling.
- Appraise the legal and regulatory compliance requirements related to Information Assurance and Information Systems Security and assess the social, ethical, economic, and technical impact of information systems security.
- Analyze the challenges encountered in establishing information systems security, information assurance, and business continuity.
- Examine the models and methodologies for performing security vulnerability assessment and risk mitigation; also analyze the principles and practices for appraising and certifying systems security.

Concentration Requirements (15 semester hours)

Code	Title	Semester Hours
ISSC641	Telecommunications and Network Security	3
ISSC642	Intrusion Detection and Incident Handling	3
ISSC660	Information Assurance	3
ISSC661	Information Assurance: Assessment and Evaluation	3
ISSC662	Information Assurance: Capability Maturity and Appraisals	3
Total Semester Hours		15

Concentration in IT Project Management (15 semester hours)

The world of Information Technology is replete with projects that were abandoned because of runaway scope and cost. On the other hand, the trend in the world economy is shrinking budgets and shorter deadline, all this while projects are getting more complex. This concentration focuses on meeting industry needs for IT Managers that can manage cost, time, scope, quality, risk, and people to ensure that projects come in on time and under budget. It also addresses strategic planning and business systems analysis.

Objectives

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

- Appraise the principles and practices for organizing, allocating, and managing project resources.
- Analyze the project management framework, including the stakeholders, domains, phases, processes, integration, and lifecycle.
- Examine the potential complexities and pitfalls in initiating and closing projects; and assess methods to mitigate this risk.
- Appraise the unique challenges in managing the scope, time, and cost of Information Technology projects.
- Examine various project cost models; also analyze the principles of earned value management (EVM).
- Assess the principles, strategies, challenges, and measures for managing quality and risk on IT projects.
- Analyze the phases, procedures, deliverables, and best practices for business systems analysis.

Concentration Requirements (15 semester hours)

Code	Title	Semester Hours
ITMG625	IT Project Management: Integration, Scope and Time	3
ITMG630	Project Management for e-Business	3
ITMG636	IT Project Management: Developing Project Schedule	3
ITMG637	IT Project Management: The Integrated Project Plan	3
ITMG638	IT Project Management: Execution, Monitoring and Control	3
Total Semester Hours		15

Final Program Requirements (3 semester hours)

Code	Title	Semester Hours
Select 1 course from the following:		3
ITCC697	Creative Project Capstone [1]	
ITCC698	Information Technology Capstone [1]	
Total Semester Hours		3

[1] Taken once all other requirements have been met.