

Information Technology Auditing and Cyber Security (M.S.)

About The Program:

The M.S. in Information Technology Auditing and Cyber Security (MS ITACS) program prepares students for cyber security, information security, information systems auditing, and IT risk management positions in business and critical infrastructure sectors of the economy identified by the U.S. Department of Homeland Security. The MS ITACS is a science, technology, engineering, and math (STEM) program aligned with the ISACA® Model Curriculum for Information System Audit and Control, which enables our graduates to earn one year of work experience applicable toward the Certified Information Systems Auditor (CISA) designation.

MS ITACS students take four common core courses and specialized courses in one of two concentrations: Information Technology Auditing or Cyber Security. The IT Auditing concentration culminates in a capstone course leading to CISA certification, while the capstone course for the Cyber Security concentration leads to Certified Information Systems Security Professional (CISSP®) certification, depending on the student's work experience. Qualified students with necessary prerequisites are able to take courses from both concentrations.

Career Options: The MS ITACS degree prepares graduates for employment in cyber security, information security, information systems auditing, and IT risk management positions at accounting and consulting firms, banks and financial companies, businesses producing goods and providing services, computer software and hardware companies, information and data service providers, and governmental agencies and non-governmental organizations. The U.S. Bureau of Labor Statistics reports 28% job growth through 2026.

Affiliation(s): Research is supported by Fox School of Business and Management's Advanta Center for Research in Financial Institutions, Center for Healthcare Research and Management, Innovation and Entrepreneurship Institute, and Institute of Global Management Studies. Research interests of the Fox School faculty are also supported by numerous centers and institutes throughout Temple University.

Areas of Specialization:

Two areas of concentration are offered:

- Cyber Security
- Information Technology Auditing

Requirements of Programs:

- **Total Credit Hours:** 30
- **Culminating Events:** The MS ITACS program culminates in a capstone that prepares students to take the appropriate professional certification examination:
 - a. Certified Information Systems Auditor (CISA)

- b. Certified Information Systems Security Professional (CISSP®), with a minimum of five years' experience

Core Courses (Information Technology Auditing Concentration)

IT Governance – Understanding how IT organizations are structured and managed is essential to effective IT auditing. In this course students will learn how IT organizations are managed and the issues which make IT management so challenging. Students will learn how strategic planning is performed within IT organizations. A number of tools, techniques, and frameworks such as COBIT will be discussed which will help make the auditor effective in this environment.

Protection of Information Assets – Information is an organization's most precious asset. Inadvertent disclosure of sensitive information can have significant operational and financial impact on the organization. Loss of information or access to it can also have serious adverse impacts on the organization. In this course students learn the importance of managing the information assets of the organization including logical IT security, physical, and environmental security. Disaster recovery and mitigating risk through insurance are also discussed.

Security Architecture – Examines the methodology by which an organization aligns its business strategy with its security operations. Both the current and desired future states of the business' security efforts are described so that resources can be directed to the security efforts most needed to support the business.

Business Skills for ITACS Professionals (2 terms) – In this course students practice a variety of business skills that are necessary to be effective as an IT auditor. These skills include managerial communications and public speaking skills, interviewing skills, negotiation and personal selling skills, business writing, industrial psychology/behavioral science skills, project/time management and team building skills. The course is delivered through a series of workshops and simulations and include observations of business practices at host IT companies.

IT Auditing Concentration Courses

IT Audit Process – This course introduces students to the essential concepts of IT auditing. Students will learn standards and guidelines for performing an IT audit. Topics will include concepts of internal controls. Students will learn to plan and manage an audit as well as how to report on evidence collected during the audit.

Systems and Infrastructure Lifecycle Management 1 – Examines how an organization builds an enterprise architecture within an environment of internal control. Topics cover include information system planning, management and usage, the development, acquisition and maintenance of these technologies and their impact on the organization's business processes.

IT Service Delivery and Support – Learn how the operational aspects of an IT organization deliver on the value proposition of the organization. Learn about the technical infrastructure and how this infrastructure provides a reliable and secure platform for applications. Learn about service center management and how these teams are utilized to deliver value to the organization.

IT Auditing Concentration Courses

Select two from the following:

Enterprise Resource Planning Systems – This course introduces students to the essential concepts of an ERP. The course looks at how a business' key transactions are executed and accounted for in an ERP. IS and accounting controls to assure confidentiality, integrity and authenticity are examined. Finally, the course looks at how transaction processing data is transformed into data for management analysis and legal entity reporting.

Special Topics

Independent Study

Data Analytics for IT Auditors – MIS 5208 examines the emerging approach of continuous-audit. This approach relies heavily on data analytics to examine datasets produced by audit and security controls (for instance, network log files). Basic data analysis concepts are presented and then applied to security or audit problems. Audit specific tools like ACL will be used in addition to general tools like Excel.

IT Auditing Capstone Course

IT Auditing Capstone – In this course students are given the opportunity to demonstrate the capabilities they have developed in other portions of the program. This course makes extensive use of case studies and role playing exercises. Students will explore a comprehensive case study which exposes them to each of the domains covered in the curriculum.

Core Courses (Cyber Security Concentration)

IT Governance – Understanding how IT organizations are structured and managed is essential to effective IT auditing. In this course students will learn how IT organizations are managed and the issues which make IT management so challenging. Students will learn how strategic planning is performed within IT organizations. A number of tools, techniques, and frameworks such as COBIT will be discussed which will help make the auditor effective in this environment.

Protection of Information Assets – Information is an organization's most precious asset. Inadvertent disclosure of sensitive information can have significant operational and financial impact on the organization. Loss of information or access to it can also have serious adverse impacts on the organization. In this course students learn the importance of managing the information assets of the organization including logical IT security, physical, and environmental security. Disaster recovery and mitigating risk through insurance are also discussed.

Security Architecture – Examines the methodology by which an organization aligns its business strategy with its security operations. Both the current and desired future states of the business' security efforts are described so that resources can be directed to the security efforts most needed to support the business.

Business Skills for ITACS Professionals (2 terms) – In this course students practice a variety of business skills that are necessary to be effective as an IT auditor. These skills include managerial communications and public speaking skills, interviewing skills, negotiation and personal selling skills, business writing, industrial psychology/behavioral science skills, project/time management and team building skills. The course is delivered through a series of workshops and simulations and include observations of business practices at host IT companies.

Cyber Security Concentration Courses

Securing Digital Infrastructure – This course examines issues related to securing the components of a company's infrastructure. It reviews network, firewall, and basic operating system security issues. It presents the material theoretically and practically through many in class and homework exercises.

Ethical Hacking – This course introduces students to the hacking strategies and tactics used by ethical or "White Hat" hackers. Methods of vulnerability exploitation to be used primarily in the process of Security Penetration will be explored in theory and in hands on exercises. The course will require simple programming using Open Source scripting languages and hacking tool kits. For that reason some knowledge of and experience with computer programming is required.

Intrusion Detection & Response – While all businesses work to be as secure as possible, it is agreed that no organization can be completely secure. Preventing attacks, quickly identifying successful attacks, detecting advanced persistent threats and monitoring systems activity in order to deter intrusions can result in significant business benefit. This course examines the variety of tools and techniques used to do this work.

Operation System Security – This course introduces students to operating system security and tools to secure and audit an organization's computer operating systems. Methods of securing operating systems will be explored in theory and through hands on exercises. The course will teach students programming techniques and how to use specific operating system and Open Source scripting languages. Knowledge of and experience with introductory computer programming is required, as is demonstrated ability to use operating systems and navigate file systems in Microsoft Windows and/or Linux is required. In this course, we will focus on securing operating systems. The first part of the course will focus on processes used to secure the MS Windows operating system. The second part of the course will apply those same techniques to the Linux operating system. The course will discuss techniques and tools used to help reduce weaknesses in default installations/configurations of different operating systems.

Cyber Security Elective Course

Select one from the following:

Special Topics

Independent Study

Penetration Testing – This course introduces students to Penetration Testing. Methods of vulnerability assessment and exploitation are examined as a means of identifying areas requiring improved security

and recommended changes. The ethical, business governance and legal implications of penetration testing are examined. Specific techniques are examined in detail with the intent of giving the students a practical understanding of how Penetration Tests are conducted and laboratory-based experience in their actual conduct.

Organizational Forensics – The focus of the course is on helping students gain a broad understanding of the field of study and how technology and law interact to form forensic science. Students will learn how computer forensics techniques are used to investigate digital data to gather evidence relating to criminal or other legal incidents and events. This course helps students understand how to find vulnerabilities, discover intrusions and respond to computer incidents. Students will learn how attackers undermine and exploit systems so they can help prepare an organization to detect and respond to them. Legal issues involved in responding to computer attacks are explored, including employee monitoring, working with law enforcement and handling evidence. Students will learn how to prepare to handle incidents, and participate in the process of incident identification, containment, eradication, recovery and lessons learned.

Cyber Security Capstone Course

Cyber Security Capstone – This is the final course in the ITACS cyber security track. The course has two purposes. First, it reviews all of the topics covered in earlier courses and further prepares the students for the SSCP exam. Second, it requires students to integrate what they have learned and research an emerging topic in the field of IT assurance.

Courses:

Click [HERE](#) for more information on the courses below.

- Information Technology Management
- Business Intelligence
- Process Improvement and Innovation
- Network Architectures for Business
- Network Centric Applica
- Object Oriented Computing
- Knowledge Mgmt/Bus Intel
- Digital Business Strategy
- User Interface Design
- Business Design and Innovation
- Enterprise Resource Planning Systems
- Enterprise Architecture for IT Auditors
- Business Essentials for IT Audits
- Inf Sys Applications-Org
- Database Mgt Sys & Model
- Sys Anal/Rapid App Dev
- Inf Tech Prin-Network-BS
- Special Topics
- Inf Architect & Network
- Inf Systems Mgt & Proces
- Independent Study
- Special Topics in MIS
- IT Audit Process
- IT Governance
- Systems and Infrastructure Lifecycle Management 1
- Systems and Infrastructure Lifecycle Management 2
- IT Service Delivery and Support
- Protection of Information Assets
- Data Analytics for IT Auditors
- Securing Digital Infrastructure
- Ethical Hacking

- Penetration Testing
- Intrusion Detection & Response
- Security Architecture
- Operation System Security
- Organizational Forensics
- Business Skills for ITACS Professionals
- Data Analytics for Management
- Managing Technology & Systems
- Design Inquiry and Research
- Data Analytics for Management
- Managing Technology & Systems
- Design Inquiry and Research
- Database Analytics
- Applied Predictive Analytics
- Social Media Innovation
- Digital Innovation in Marketing Capstone
- Managing Information
- Special Topics
- Capstone in Information Technology
- IT Auditing Capstone
- Cyber Security Capstone
- Qual & Interpret Meth-IS
- Foundations of Electronic Commerce Research
- Adv Research Methods-IS
- Proseminar in Management Information Systems
- Contemp Topics & Res-IS
- Directed Study in MIS