



2004-2005 Catalog Addendum

New Program

Master of Science in Information Assurance

This Walsh College Master of Science in Information Assurance degree combines theory with applied learning enabling security practitioners to be functional upon completing the degree. The program is designed to meet the high demand for information assurance professionals in government, corporations and industry.

The Walsh MSIA allows students to choose specializations that fit their professional goals. Students whose undergraduate work was in accounting or finance may wish to pursue the audit track and prepare for the CISA certification offered by the ISACA. Students who wish to focus their careers in law enforcement will find the digital forensics track will meet their needs. Executives and high level managers who plan to be information assurance decision-makers will prefer the rigorous chief information security officer track.

Admission Requirements

- Posses an undergraduate degree or higher in Management Information Systems or Computer Information Systems or equivalent forma college or university accredited by the Higher Learning Commission of the North Central Association of Colleges and Schools or one of the following regional associations: Middle States, New England, Northwest, Southern, or Western.
- Have an overall cumulative grade point average of 2.750 or better on a 4.000 scale (for applicants with less than a 2.750 GPA see the provisional status section in the online Walsh College Catalog.
- Documentation of two years successful experience (may be in process, but must be completed prior to degree or certification completion)
- Appropriate basic level of educational/skills assessment in the area of computer security or internetworking.

Program Format

The Master of Science in Information Assurance (MSIA) program consists of five foundation courses that may be taken at Walsh College or excluded, depending on a student's prior education, certifications and/or experience. The program consists of:

- Foundation courses (5 courses for 15 credit hours; individuals who have the CISSP certification will be waived from the foundation courses).
- Core Courses (8 courses for 24 credits)
- Specialization (4 courses for 12 credits)

Foundation

BIT	546	Introduction to Information Systems Security
BIT	571	Establishing and Information Protection Plan
BIT	572	Security Safeguards
BIT	573	Threat Assessment
BIT	574	Introduction to Cryptography

Core Courses

IA	500	Seminar on public Sector Security Issues
IA	510	Secure System Architecture and Design
IA	520	Ethics and Legal Issues for Security Practitioners
IA	530	Authentication Technologies and Standards
IA	540	Intrusion Technologies and Standards
IA	545	Physical Security
IA	547	Seminar on Business Continuity Planning
IA	590	Information Assurance Capstone

Specializations

Digital Forensics

IA	551	The Law and Digital Crime
IA	552	Introduction to Structured Digital Forensics
IA	553	Conducting a Cyber Crime Investigation I
IA	554	Conducting a Cyber Crime Investigation II

Audit

IA	561	Introduction to Auditing Models
IA	562	Auditing Computer Systems I
IA	563	Auditing Computer Systems II

IA 564 Conducting and Audit

Chief Information Security Officer (CISO)

BIT 561 Fundamentals of Project Management

MBA 501 Management and Organization

COM 540 Strategic Management

IA 570 CISO Skills

MSIA Course Descriptions

IA 500 Seminar on Public Sector Security Issues

The federal government is developing many stands and practices for security practitioners to follow if they work with federal, state or local government electronic assets. This class will examine the certifications, accreditation processes and regulations imposed by the federal government for security professionals to follow. Lectures, special projects and business case analysis will be utilized by the students to learn the material.

IA 510 Secure System Architecture and Design

This class will focus on advanced architecture and design concepts for large, heterogeneous networks, as well as special design issues for specific technologies such as virus controls, DDoS, Identity Management, Intrusion Prevention, VOIP, Convergence and other current technology advancements. Lab work will be heavily emphasized in this class to help the student grasp the concepts.

IA 520 Ethics and Legal Issues for Security Practitioners

This session will build on the experiences obtained in the previous security classes in order to challenge students to apply proper behavioral responses to challenging “real-world” situations. Business case study and group projects will explore the issue of ethical challenges and legal issues that face security practitioners. This class will show students how to understand and evaluate the impact of these legal and ethical issues on their ability to do their jobs responsibly. Privacy and security legal issues will be explored, along with specific regulations such as HIPAA, GLBA, Sarbanes-Oxley, Patriot Act, FISMA, GISRA and others. Techniques for planning, managing and implementing strategies based on these regulatory requirements will be discussed.

IA 530 Authentication Technologies and Standards

Authentication and encryption techniques are the cornerstone for protecting electronic access to information. This class will explore in depth the capabilities and issues involved with designing and implementing various authentication and encryption schemes for security practitioners. Protocols, standards, and approaches will be explored in hands-on labs and research to provide a deep understanding of how to protect the Confidentiality, Integrity, Availability and non-repudiation of information

IA 540 Intrusion Techniques and Defenses

This session will introduce the student to common attack techniques and mitigating countermeasures. The student will gain an understanding of common attacks on web sites, database structures, Internet services, TCP/IP services, people and other important elements of an organization's infrastructure. In addition to understanding how attacks work, students will be taught how to not only recognize these attacks but to also defend themselves against such attacks. Lab Access Required.

IA 545 Physical Security

This session will focus on traditional physical security threats and countermeasures, as well as some of the newer "convergence" issues and technologies that have been developed since 9/11. Physical security mechanisms covered during this class include people, data, equipment, systems and facilities.

IA 547 Seminar on Business Continuity Planning

Ensuring a business can survive a catastrophic event is an important element of strategic planning for businesses today. This class will examine the steps needed to design, implement and test a business continuity plan. Businesses large and small also have many different legal and regulatory challenges facing them today. Executive responsibility for doing business in the electronic age will be examined as well as fraud techniques and case studies involving incident response and recovery.

IA 590 Information Assurance Capstone

This will be the final class that will be utilized to encapsulate all of the knowledge obtained during the degree process in the form of a student project.

Specialization Courses

IA 551 The Law and Digital Crime

Students will study how digital crime is committed, the different types of crime definitions and legal issues surrounding using computers to commit a crime. An overview of forensic investigation techniques will be presented, along with an overview of the process for the collection, analysis and preservation of evidence for a trial. Working with both the private and public sectors will be examined during this course (police, lawyers, corporate legal counsel, etc). A mock trial will be conducted as part of this class.

IA 552 Introduction to Structured Digital Forensics

A complete overview of the digital forensic process will be presented for students to evaluate and comprehend. Tool sets, procedures and working with law enforcement will be examined to show students how digital forensics is conducted. Case file analysis, interview techniques and court testimony (expert witness) will be covered during this class.

IA 553 Conducting a Cyber Crime Investigation I

An intermediate level class that will build upon the techniques and skills learned previously. Heavy emphasis will be placed on using techniques and tools sets to collect and analyze evidence. Forensic case studies will be performed during this class.

IA 554 Conducting a Cyber Crime Investigation II

An advanced level class that will build upon the techniques and skills learned previously. Heavy emphasis will be placed on the soft skills required to conduct an investigation, as well as working with law enforcement and lawyers to support cases. Forensic case studies will be performed during this class.

IA 561 Introduction to Auditing Models

This class introduces the student to the financial, operational and comprehensive classification of audit approaches. This class will cover the skills necessary to perform such audits that require globally-applicable standards that apply specifically to information systems auditing. An overview of the audit process will be covered through the use of business case analysis and real-world audit projects.

IA 562 Auditing Computer Systems I

Tools, techniques and processes utilized to perform an organizational IT audit will be covered. Students will go through a mock audit of an organizational IT environment and produce a final audit report.

IA 563 Auditing Computer Systems II

This class continues to add to the knowledge obtained previously. Additional tools, techniques and processes utilized to perform an organizational IT audit will be covered. Students will go through a mock audit of an organizational IT environment and produce a final audit report.

IA 564 Conducting an Audit

Students will be presented with a case study for an organization and will have the semester to perform an actual audit. Auditing procedure will be covered and documented, as will the approaches used to finalize any recommendations as an outcome. This session builds upon the previous classes and provides the student a mechanism to apply all of the techniques learned.

BIT 561 Fundamentals of Project Management

This course serves as an introduction to the generally accepted processes and knowledge areas found within the project management profession. Students will be introduced to the project management concepts as defined by the Project Management Body of Knowledge © (PMBOK). Topics covered include the nine project management knowledge areas as well as the domains of initiating, planning, execution, controlling, and closing of projects. Professionalism and ethics are emphasized. Case studies are used to illustrate the concepts and students will work individually and in teams to initiate, plan, execute, control, and close projects. Students will learn the use of Microsoft Project to develop and manage project plans.

MBA 501 Management and Organization

This course explores the functions, roles and skills associated with managing people and organizations. Students study the foundations of individual and group behaviors as well as the concepts and models for effective management. Students also examine the

structure and processes of organizations with an emphasis on the leadership required to manage the dynamics involved. Critical thinking, decision-making, ethics, and organization culture are recurring themes in this course.

COM 540 Strategic Communication

Prerequisite: MBA 501

This course involves students in the elements of message design, creation, and transmission of various modes of business communications. Students will examine and differentiate forms of authoring while building communication skills for internal and external audiences. Varying formats will include document types such as marketing, crisis communication, image and mission, and social responsibility as well as customer documents, compliance auditing, digital documentation, newspaper releases, training materials, and other media and business documentation. Composition guidelines will be provided and used in developing various messages. The design of persuasive, informational, narrative and other categories of organizational messages are studied and practiced.

IA 570 CISO Skills

This final class in the CISO track will examine issues faced by CISO's everyday. Guest lectures and speakers from industry will be utilized in combination with lectures, business case study and special projects to learn the skills CISO's need to excel at their jobs.