



INFORMATION ASSURANCE

Director: Dan Shoemaker
Office: Briggs 344
McNichols Campus
Telephone: (313) 993-1287
Fax: (313) 993-1166
E-mail: shoemadp@udmercy.edu
Website:
<http://liberalarts.udmercy.edu/programs/depts/information-assurance/index.htm>

The Master of Science degree in Information Assurance (MS-IA) is a multidisciplinary, 30-credit hour graduate degree. It is designed to produce a comprehensively educated information assurance professional. It will be taught by professors in three UDM Colleges. The aim is to produce rigorously educated leaders to engage in the serious business of protecting the nation's information infrastructure.

Protection of America's critical infrastructure is an emerging national priority. Due to its implications for national security, the responsibility for this program has been placed jointly with the National Security Agency (NSA) and the U.S. Department of Homeland Security.

Universities who meet the rigorous criteria established by these two federal agencies are granted designations as Centers of Excellence in IA education. This is a highly competitive annual process involving rigorous review of the target curriculum by national experts.

The curriculum of the University of Detroit Mercy received its Center of Excellence (CAE/IAE) award at West Point on June 8, 2004. This is a national distinction. There are only 67 Centers of Excellence among the over 3,000 colleges and universities in the United States. Moreover, only universities that have been designated by this process are eligible to participate in the IA training and education programs funded by the federal government.

Interdisciplinary Approach

The Joint IA degree is the first curriculum that embodies content taught by professors in three different colleges and as such, it is the national model for advanced interdisciplinary IA programs. Information Assurance professionals have to know about advanced technology in order to keep computer networks secure. However, it is equally important to build a secure staff and organizational system that will protect the integrity of the data. UDM teaches students to put together a total solution.

Ethical conduct, legal and regulatory compliance, and strategic policy all must be considered. These considerations all have to be bundled together in a single seamless solution,

which is properly attuned to the threat to the environment and which reflects resources and capabilities.

At other universities, knowledge about how to select staff and secure the physical facility is provided by professors whose expertise is actually in technology. UDM will call on professors from other fields to provide a comprehensive approach to all aspects of the problem

Admissions Requirements

Admission decisions are made based on GPA, undergraduate major, work experience, and other degrees.

Degree Requirements

Joint IA Degree - Perpetual Schedule

Fall

- [CIS 5570 - Networks](#)
- [CIS 5700 - Information Security Principles](#)
- [SEC 5560 - Terrorism and Homeland Security](#)
- [CIS 5590 - Network Security \(requires 5570\)](#)

Winter

- [CIS 5750 - Information Assurance Management \(requires 5700\)](#)
- [SEC 5870 - Physical and Personnel Security](#)
- [Select Capstone](#)
- [CIS 5300 - Software Assurance](#)

Spring/Summer

- [CIS 5580 - System Forensics \(requires 5700\)](#)
- [CIS 5790 - Assurance Processes \(requires 5750\)](#)
- [Complete Capstone](#)

NOTE: Courses with an asterisk denote the CNSS Certificate.



For further information, please write, call or e-mail:

Dan Shoemaker, Program Director
 University of Detroit Mercy
 4001 W. McNichols Rd.
 Detroit, MI 48221-3038
 shoemadp@udmercy.edu
 (313) 993-1287
 or
 Theresa Carson
 Graduate Admissions Counselor
 carsonta@udmercy.edu
 (313) 993-3309

International Students: contact Steven Coddington at coddinism@udmercy.edu or (313) 993-3310

Overall Course Descriptions**CIS 5300 Software Assurance 3 cr.**

(Prerequisite: Completion of pre-core requirements and CIS 5200.)
 Qualifies for CNSS certification. Management of a quality system in software production. SQA Standards (ISO, IEEE) and best practices (CMM, SPICE.) Comprehensive coverage of Unit, Module, System, and Acceptance Testint. Principles, methods, models, standards and software tools used in the process of testing.

CIS 5570 Networks 3 cr.

Qualifies for CNSS Certification. An examination of standardization and design issues for the communication infrastructure. Topics include: Communication hardware and software, standards and protocols (like: OSVISO and TCP/IP.) LAN, EDI. Special emphasis will be placed on recent advances, network administration and ensuring security of networks and transmitted data.

CIS 5580 Systems Forensics 3 cr.

(Prerequisite: Permission of instructor.)
 This course presents the legal concerns, investigation techniques and incident response tactics of forensic investigation and forensic auditing. It centers around the basic operating system concepts that underlie this area. Students will learn evidence gathering and presentation techniques based around the Windows Incident Response Collection Report (IRCR). They will also learn how to employ IDS and CERT for effective incident response. Students will study the real-world investigation issues and concepts developed through the Honeynet Project.

CIS 5590 Network Security 3 cr.

Qualifies for CNSS Certification. This course offers an in-depth understanding of the concepts, principles and practices of network and electronic data security as well as all relevant industry standards. Topics include classic methods for the

identification analysis, design and response to network security incidents, in addition to an introduction to the principle set of issues involved with electronic data protection such as pen testing and automated methods for assuring data integrity, confidentiality and availability.

CIS 5700 Information Assurance 3 cr.

(Prerequisite: Permission of the instructor.)

This course presents an overview of the multidisciplinary process of information assurance. It is rooted in the information assurance body of knowledge (IBOK). The student will learn about the issues involved in creating a systematic information assurance control structure, how to establish systematic security auditing and control procedures and how to build systematic information assurance capability into the IT function.

CIS 5750 Information Security Management 3 cr.

(Prerequisite: Permission of the instructor.)

The purpose of this course is to educate students in the discipline of information security management. Students will learn how to establish and maintain a systematic security solution for a business organization as well as build systematic information accounting procedures into normal operation. The focus is purely operational best practice rather than theoretical. The outcome will be a fully certifiable information security management system (ISMS).

SEC 5560 Terrorism and Homeland Security 3 cr.

Throughout history terrorists have utilized violence to spread fear throughout a population in order to serve political or other more amorphous purposes. This course will examine the history, forms strategies and tactics of terrorism as well as its sociology, psychology and criminology. Terrorist profiling along with the problems of false positives and false negatives will be explored. Counterterrorist efforts by the Department of Homeland Security as well as by state and local governments will be evaluated. Private sector defense of the nation's critical infrastructure will also be studied.

SEC 5870 Physical and Personnel Security 3 cr.

Together with information security, physical and personnel security defend the critical infrastructure against cyberterrorism, terrorist and conventional criminal attack. Physical security involves the protection of assets through the use of security awareness, training, intrusion detection systems, environmental controls and human prevention and intervention activities. Personnel security ensures that an organization's employees have been screened, vetted, selected and supervised to maximize their fidelity to organizational and national goals as well as their own personal and professional growth. Both physical and personnel security are multidisciplinary in nature and must be effectively implemented within the legal framework of a democratic society.