Information Assurance Education and the IS Curriculum

Kevin Lee Elder,   Dennis Strouble,   Dave Bouvin
Air Force Institute of Technology
Wright Patterson AFB, Ohio 45433, USA

Abstract

In this paper we will summarize the recent efforts of the Graduate Information Resource Management (IRM) program at the Air Force Institute of Technology to offer a specialization/track in Information Assurance to our students taught from an IRM perspective. This program is built off of the National Security Agency's (NSA) 4012 Certification for Information Assurance. The NSA has identified sixty Centers of Excellence in Information Assurance Education. The majority of the Centers are primarily housed in Computer Science Departments or the courses offered are primarily taught by Computer Science Faculty (45 out of 60).   By mapping our curriculum to the certification requirements for the NSA 4012 and mapping those to the knowledge clusters within the course's learning objectives using the Maconachy Model we believe we have an interesting and robust Information Assurance Curriculum that others may want to compare to and investigate.

Keywords: information assurance, education, curriculum

1.   INTRODUCTION

At the Graduate School of Engineering and Management, Department of Systems and Engineering Management, we have been performing Information Assurance education for several years. In this paper we will summarize the recent efforts of the Graduate Information Resource Management (IRM) program to offer a specialization/track in Information Assurance to our students taught from an IRM perspective. This program is built off of the National Security Agency's (NSA) 4012 Certification for Information Assurance (NSTISSI, 1997). This program does not build off of the existing NSA 4011 Certification (NSTISSI, 1994) offered in the Computer Science Department.

With the ever increasing emphasis in the area of Information Superiority being experienced in the DoD, the school is a stage of rapid growth in size. The concepts of Information Superiority and Information Warfare are somewhat unique to the DoD. However, we feel other schools could benefit from seeing a review of our program to meet our unique needs in the area of Information Assurance. Most businesses and industry face similar if not identical situations. Other schools might need to adapt in a similar manner to face the demands placed on their future IS graduates.

2.   BACKGROUND OF INFORMATION ASSURANCE

The National Security Agency's (NSA) Information Security Assessment Model (IAM) identifies 18 baseline categories that should be included as components of the Information Assurance (IA) posture of any organization (Hurd, 2001):

These categories are generally accepted when developing and maintaining systems under the information technology (IT) realm (Swanson, 1996). Even though there are several organizations that provide justification of important categories, the NSA IAM was developed specifically for government and commercial organizations and is often referred to as the accepted standard for IA related system certifications to enhance the protection of information and the establishment of functional IA programs (Hurd, 2001; 256).

Table 1: NAS IAM 18 Baseline Categories (Hurd, 2001)

1	IA Documentation
2	IA Roles and Responsibilities
3	Identification & Authentication
4	Account Management
5	Session controls
6	External Connectivity
7	Telecommunications
8	Auditing
9	Virus Protection
10	Contingency Planning
11	Maintenance
12	Configuration Management

13	Back-Ups
14	Labeling
15	Media Sanitization/Disposal
16	Physical Environment
17	Personnel Security
18	Training and Awareness

A limited number of models dedicated to the understanding of threats to automated information systems are currently available. The McCumber (1998) model is used to appropriately organize the 18 baseline categories for analysis and to address the possible threats to automated systems. This comprehensive model addresses threats and functions as an assessment and evaluation tool. McCumber argues that it is a key concept because it is independent of technology and is not constrained by organizational differences and thus can be used for systems development. The three dimensions focus on information states, critical information characteristics, and security countermeasures. Maconachy et al (2001) expanded the McCumber model to include the theory that we are now in an information intensive environment, which broadens the scope and the overall understanding of information and systems protection. The strength of the multidisciplinary and multidimensional elements of the McCumber model is in its ability to produce or maintain a robust IA program. Figure 1 shows this model and demonstrates an integrated approach that accounts for three of the four dimensions of IA, information states, security services, and security countermeasures.
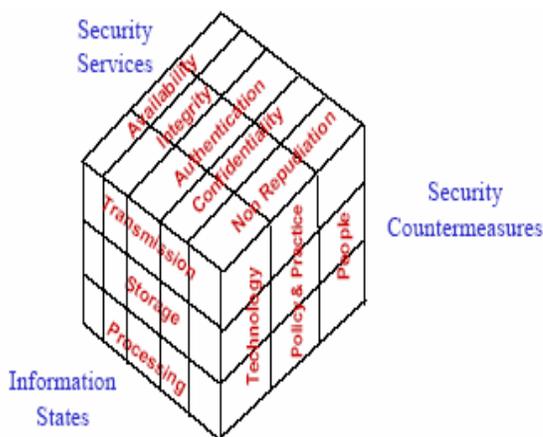

Figure 1: Information Assurance Model
(Maconachy et al, 2001)

Additionally, Maconachy et al created a fourth dimension, time. The time dimension of the integrated model demonstrates the introduction of new technology over time requires modifications to other dimensions of the integrated model in order to restore a system to a secure state of operation. This dimension is related to the notion that certain aspects of the McCumber model has changed with innovation and is essential to the theory that IA throughout military operations in warfare has evolved from earlier concepts. Essential elemental changes over time were fundamental to the adoption of new technology or doctrinal enhancements that were evident during military conflicts. Such changes to the system over time were key aspects of restoring a secure state.

Using a current framework such as the Maconachy et al (2001) model to evaluate past occurrences will provide evidence about whether the concept currently known as IA is valid for earlier U.S. Military conflicts. A modified list of the baseline categories are grouped in Table 2 below using the Maconachy (2001) model. This grouping will form the foundation for the evolutionary model that will be used to map the knowledge into our research effort.

Each category has specific questions or pertinent information that should be included when conducting an Information Assurance assessment and should be included in an Information Assurance curriculum.

3. NSA CENTERS OF EXCELLENCE IN INFORMATION ASSURANCE EDUCATION

The National Security Agency's (NSA) has identified sixty Centers of Excellence in Information Assurance Education as listed in Appendix 1. The majority of the Centers are primarily housed in Computer Science Departments or the courses offered are primarily taught by Computer Science Faculty (45 out of 60). Only 15 out of 60 primarily utilize faculty from outside of Computer Science in Information oriented programs. Only 22 of the 60 centers offer the NSA 4012 certification. Furthermore, only 8 of those 22 centers offer the 4012 certification with a curriculum taught from an Information program. Additionally, almost all of those eight centers build the 4012 off of the 4011 certification. In our program we will not build off of the 4011 certification, the 4012 will stand alone. The majority of the courses (and all that are required) are taught in the Information program. Any school interested in starting an information assurance program should look through this list of programs. Any school outside of a computer science program would most likely be interested in reviewing our program.

Table 2: IA Model - NSA IAM Mapping (Hurd, 2001)

IA Model Dimensions	NSA IAM Baseline Categories
Information States	
Transmission	External Connectivity
Storage	Back-Ups Disposal
Processing	Auditing Session Controls
Security Counter Measures	
Technology	Maintenance Telecommunications Virus Protection
Policies and Practices	Account Management Configuration Management Contingency Planning IA Documentation IA Roles & Responsibilities Media Sanitization
People	Awareness Personnel Security Physical Security Training

4. IRM PROGRAM DESCRIPTION

The Graduate School of Engineering and Management, Department of Systems and Engineering Management, offers the Master of Science in Information Resource Management (IRM) with options for a concentration of study in strategic information management, information assurance, database systems, and/or computer networks This program is designed to provide students with the knowledge and skills needed to oversee both the information management and information systems needs of Air Force, DoD, and allied military organizations in future assignments as middle and upper-level managers. The program is designed primarily to reflect the needs of the officer and enlisted members of the Air Force communications and information officer career field; however, it is currently open to members of other career fields as well. In order to address the requirements associated with the growing importance of "information" as a critical resource for all career fields, the program continues to expand as necessary to serve a new customer base.

Overall, the IRM program provides students with a broad perspective of DoD information-related issues, including information strategy, information architec-tures, information security, information ethics, information system design/development/acquisition and related business process support, and the individual and organizational implications of rapidly evolving information technology. During the recent years, the program has also expanded to examine knowledge, in addition to information, as a critical organization resource. One can think of information as that which is gathered, stored, and disseminated through on organization's myriad information systems. Knowledge, the product of that information, is that which resides in the heads of the organizational decision makers. Ultimately, it is the knowledge's support for decision making that is the reason for gathering, storing, and disseminating organizational information. The focus is on improving the student's understanding of, and ability to manage information/knowledge in, today's dynamic information technology and global environment.

All graduates of the IRM program at the Air Force Institute of Technology should be able to:

- Use effective oral and written communications.
- Understand and apply concepts and techniques of descriptive and inferential statistics to analyze problems under conditions of risk and uncertainty.
- Understand and apply the concepts, methods, and tools related to planning, directing, and controlling resources (financial, human, information/knowledge, and capital) in an information resource management context.
- Understand how to take advantage of information and knowledge as a resource to improve organizational effectiveness, efficiency, and ultimately competitive advantage.
- Know how information technology affects information and knowledge as a resource and how it may modify existing organizational structure and working relationships.
- Learn to examine processes from beginning to end by employing innovative technologies and organizational resources.
- Learn to conduct strategic information planning to link the management of information, knowledge, information architectures, information technology, and systems to an organizations' strategic business goals.
- Conduct and present methodical research to solve problems and support decisions.

The IRM/ISM programs are conducted in six academic quarters and a short term (18 total months) for DoD-sponsored full-time students. The short term provides an orientation to the IRM program, an introduction to the curriculum options, and a review of basic writing and mathematics skills. The minimum curriculum satisfying the degree requirements consists of 2 management core courses, 6 IRM/ISM core courses, 1 research methods course, 2 statistics courses and 12 hours of thesis

research. Prerequisite course requirements are noted in the section below. The management core courses provide important knowledge in areas that are fundamental to the study of information resource management. The management core courses include:

ORSC 542 Managerial Behavior in Organizations
EMGT 530 Contract Management.

The IRM/ISM core courses provide a thorough grounding in the concepts of information resource/systems management. The IRM/ISM core courses include:

IMGT 530 Conceptual Foundations of IRM
IMGT 580 Enterprise Information Architecture
IMGT 561 Database Management
IMGT 651 Systems Analysis and Design
IMGT 657 Data Communications
IMGT 690 Capstone Seminar in IRM.

The research methods and statistics courses provide depth of study on techniques for accomplishing academic research. Both quantitative and qualitative research methods are covered in these courses. The thesis research, which must address a problem in an information resource management or closely related area, provides the student an opportunity to draw on the concepts of the IRM course work and to demonstrate a mastery of one research methodology in pursuit of a research question. Typically, thesis topics are provided by DoD/USAF agencies interested in sponsoring student research in areas of practical concern. Specific elective courses may be required by the thesis advisor to adequately prepare for the required thesis research. Additionally, in accordance with customer guidance, quota students are highly recommended to take OPER 501, Quantitative Decision Making, if their academic schedule allows.

5.   INFORMATION ASSURANCE TRACK

Students must choose a 3 to 4-course concentration from alternatives established by the IRM faculty. Generally, IRM students can select any of the concentration sequences. IRM students with more advanced math backgrounds may be more qualified for the technically-oriented sequences, Database Systems or Computer Networks; however, this can be discussed with a faculty advisor and decided on a case-by-case basis. Students may also elect to combine two different concentrations; for the most part, the class schedules are generally established in such a way as to support this dual concentration option. Each sequence will present a unified direction and purpose and will build depth in a specific academic area related to the student's academic interests. Elective courses and additional coursework are offered and are designed to broaden the student's horizons and/or provide more in-depth knowledge in a specific area of interest.

Both Joint Vision 2010 and Joint Vision 2020 recognize the information sphere as the fifth realm of modern day warfare. Information superiority is the "capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same" (Joint Chiefs of Staff, 2000). Jobs differ widely according to the requirements of the task. The information assurance (IA) concentration provides exposure and knowledge of information security and resources management for those seeking leadership positions responsible for the management of information. All students successfully completing these three courses (i.e., with a B or better in each course) will receive a Certificate for Information Systems Security Professionals under the National Training Standard NSTISSI No. 4012 from the National Security Agency (NSTISSI, 1997). This sequence consists of the following 3 courses:

IMGT 684 Strategic Information Management
IMGT 688 Security and Ethics in the Information Age
IMGT 687 Managerial Aspects of Information Warfare.

Students begin the Information Assurance sequence with a comprehensive introduction to information warfare, management information systems, computer networking, data communications, data and information security, along with principles and best practices for protecting vital information resources. This sequence provides a background in information security, theories of information warfare, psychological operations, threats to information security, hacking, and virus awareness. Students also learn the fundamentals of encryption (both conventional and public key), information deception, and deception detection in information systems among other concepts. With a strong foundation established, students go onto examine case studies in information assurance, thereby receiving an understanding of real world phenomena in this rapidly growing realm of communications and information.

Students taking the Information Assurance sequence often complete their thesis research in this area as well (however, this is not mandatory). Electives provide students with opportunities for exploration of related topics to the IA field. Topic areas such as security, ethics, and leadership offer students key insight into specific subsets of IA. The IA curriculum complements the IRM and management core courses by building on concepts derived from research and successful practices.

Suggested Electives Related to the Information Assurance Sequence are:

CSCE 525 Intro to Information Warfare
CSCE 625 Info Sys Security, Assurance and Analysis I
CSCE 725 Info Sys Security, Assurance and Analysis II
IMGT 570 E-Business
IMGT 680 Knowledge Management
SENG 530 Introduction to Space Operation

ORSC 638 Seminar in Contemporary Leadership
ORSC 647 Organizational Policy and Strategic Mgt.

6. KNOWLEDGE CLUSTER MAPPING

Within the three required courses (IMGT 684, IMGT 687, and IMGT 657) the certification requirements for the NSA 4012 have been mapped to the knowledge clusters within the course's learning objectives. These clusters are listed below in table 3.

With the knowledge gained in this program the students should be prepared to perform the functions of the Designated Approving Authority (DAA) as defined in NSTISSI no. 4012 (1997):

> Granting final approval to operate an IS or network in a specified security mode
> Reviewing the accreditation documentation to confirm that the residual risk is within acceptable limits
> verifying that each IS complies with the IS security requirements, as reported by the Information Systems Security Officer (ISSO)
> ensuring the establishment, administration, and coordination of security for systems that agency, service, or command personnel or contractors operate
> ensuring that the Program Manager (PM) defines the system security requirements for acquisitions
> assigning INFOSEC responsibilities to the individuals reporting directly to the DAA approving the classification level required for applications implemented in a network environment
> approving additional security services necessary to interconnect to external systems (e.g. encryption and non-repudiation) reviewing the accreditation plan and sign the accreditation statement for the network and each IS
> defining the criticality and sensitivity levels of each IS
> reviewing the docuemetation to ensure each IS supports the security requirements as defined in the IS and network security programs
> allocating resources to achieve an acceptable level of security and to remedy security deficiencies
> establishing working groups, when necessary, to resolve issues regarding those systems requiring multiple or joint accreditation.

Table 3: IRM Knowledge Clusters

1	Legal Issues
2	Liability Issues
3	Crime Issues
4	Computer Security Policy
5	OMB Circular A-130
6	Electronic Records Management
7	Threats and Incidents
8	Threats and Vulnerabilities
9	Access
10	Administrative Responsibilities
11	COMSEC
12	Tempest
13	DAA Authority
14	Life Cycle Management
15	Continuity of Operations (COOP)
16	Risk Management

7. CONCLUSIONS

Maconachy et al (2001) model introduced the theory that we are now in an information intensive environment, which broadens the scope and the overall understanding of information and systems protection. The strength of the multidisciplinary and multidimensional elements of the McCumber model is in its ability to produce or maintain a robust IA program. By mapping our curriculum to the certification requirements for the NSA 4012 and mapping those to the knowledge clusters within the course's learning objectives using the Maconachy Model depicted in Figure 1 we believe we have an interesting and robust Information Assurance Curriculum.

This paper described the unique Masters program(s) at a Midwestern United States school that primarily serves a specific student body made up of Department of Defense employees. With a program in place for many years in Information Assurance (IA) we have now created this new program with a decidedly IRM focus to IA. It is the authors hope that other schools can use this information to review their own program(s) and incorporate the concepts presented here as appropriate. While these concepts are somewhat unique to the DoD, we feel other schools could benefit from there inclusion into the curriculum. The concept of Information Assurance is now popping up in many schools while it has been in the DoD for many more years.

8. **REFERENCES**

Hurd, Bryan, E. *"The Digital Economy and the Evolution of Information Assurance."* Proceedings of the IEEE: 252-257. June 2001.

Maconachy, William V., Corey D. Schou, Daniel Ragsdale, and Don Welch. "A Model for Information Assurance: An Integrated Approach", 2nd Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop. June 2001.

McKnight, Walter, L. *"What is Information Assurance?"* CrossTalk: July 2002. http://www.stsc.hill.af.mil/crosstalk/2002/07/_index.html.

"National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4011 – National Training Standard for Information Systems Security (INFOSEC) Professionals", June 1994.

"National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4012 – National Training Standard for Designated Approving Authority (DAA)", August 1997.

Ragsdale, Dan, Don Welch, and Ron Dodge. "Information Assurance the West Point Way." IEEE Security and Privacy:September/October 2003.

Swanson, M. and B. Guttman. *Generally Accepted Principles and Practices for Securing Information Technology Systems.* National Institute of Standards and Technology (NIST), Technology Admin, U.S. Dept. of Commerce: September 1996.

9. **APPENDIX 1 – LIST OF NSA ACADEMIC CENTERS OF EXCELLENCE**

Center of Academic Excellence	IA Training Standards
Air Force Institute of Technology	4011,4012
Auburn University	4011, 4012
Boston University	4011, 4013
Capital College	4011, 4012, 4013, 4014, 4015
Carnegie Mellon University	4011
Dakota State University	4011, 4013
Drexel University	4011, 4013
East Stroudsburg University	4011, 4012
Florida State University	4011
George Mason University	4011
George Washington University	4011, 4013, 4015
Georgia Institute of Technology	4011, 4014
Idaho State University	4011, 4012, 4013, 4014, 4015
Indiana University of Pennsylvania	4011, 4013
Information Resources Management College of the Natl. Def. Univ.	4011,4012
Iowa State University	4011
James Madison University	4011
Johns Hopkins University	4011, 4012, 4013, 4014, 4015
Kennesaw State University	4011, 4012, 4013, 4014
Mississippi State University	4011, 4014
Naval Postgraduate School	4011, 4012, 4013, 4014, 4015
New Jersey Institute of Technology	4011
New Mexico Tech	4011, 4012
North Carolina State University	Not Available
Northeastern University	4011
Norwich University	4011, 4012, 4014
Pace University	4011, 4013
Pennsylvania State University	4011, 4012
Polytechnic	Not Available
Portland State University	4011
Purdue University	4011, 4012, 4013
Stanford University	Not Available
State University of New York, Buffalo	4011
State University of New York, Stony Brook	4011
Stevens Institute of Technology	Not Available
Syracuse University	4011, 4013

Center of Academic Excellence	IA Training Standards
Texas A&M University	4011
Towson University	4011
University of California at Davis	4011
University of Dallas	4011, 4012, 4013, 4014, 4015
University of Detroit, Mercy	4011, 4012
University of Idaho	4011
University of Illinois at Urbana-Champaign	4011
University of Maryland, Baltimore County	4011, 4012
University of Maryland, University College	4011
University of Massachusetts, Amherst	Not Available
University of Nebraska at Omaha	4011, 4012, 4013
University of North Carolina, Charlotte	4011, 4013, 4014
University of North Texas	4011, 4013
University of Pennsylvania	4011
University of Pittsburgh	4011, 4012, 4013
University of Texas, Dallas	4011, 4013
University of Texas, San Antonio	4011, 4012, 4013, 4014
University of Tulsa	4011, 4012, 4013, 4014, 4015
University of Virginia	Not Available
University of Washington	4011, 4013
Walsh College	4011
West Chester University of Pennsylvania	4011, 4013
West Virginia University	4011, 4012