Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Implementing a CNSS 4012 Certification in an Information Systems Curriculum

Nary Subramanian, *The University of Texas at Tyler*, and George Whitson, *The University of Texas at Tyler*

Abstract – There has been a standard curriculum for Information Systems programs since the introduction of the DPMA Model Curriculum in 1981. Security management has been an important ingredient in all of the Information Systems curricula. For example, in the 1981 curriculum the CIS-13 course was titled EDP Audit and Controls and was taught much like it would be today, except the techniques were applied only to main-frames. The CNSS 4012 certification, for Senior Systems Managers is a natural certification to be added to an Information Systems program. This paper reviews how security management has been included in all of the model curricula up to, and including the soon to be released IS 2010 curriculum, and illustrates how to implement an CNSS 4012 certification in both an IS 2002 and IS 2010 curricula. However, this also implies that any new curricula implementation should first consider impact on satisfying the stringent requirements for CNSS certifications.

I. Introduction

Computer science began to develop as a separate discipline in the 1960's. Most of the early courses stressed programming for mathematics and engineering, but by the late 1970's many computer science teachers felt that there was a need to develop a curriculum for students primarily involved in developing business applications. In 1981, the Data Processing Management Association (DPMA) introduced its model curriculum [1]. It consisted of seven core courses and eight electives. The core was:

CIS-1 Introduction to Computer-Based Systems
CIS-2 Applications Program Development I
CIS-3 Applications program Development II
CIS-4 Systems Analysis Methods
CIS-5 Structured Systems Analysis and Design
CIS-6 Database Program Development, and
CIS-7 Applied Software Development Project.

And the electives covered other areas of business programming, including

CIS-13 EDP Audit and Controls

which was a security course offered in 1981 that was much like comparable courses today. In 1986, the DPMA '86 curriculum was introduced to reflect the introduction of the personal computer into the business world. This was accomplished by slight modifications to most of the courses and the introduction of a new course

CIS 86-2 Microcomputer Applications in Business

and a course in data center management, namely

CIS 86-7 Information Center Functions.

The Data Center Management course had many of the features of a modern security course, although network security was largely unheard of since network standards were just being introduced.

Between 1986 and 2000 several more versions of a model curricula for business were introduced that tried to capture the emergence of client/server computing. Initially, these curricula reflected an uneasy co-existence of mainframe computing with client/server, but by 2002 a new curriculum, IS 2002, was approved by Association for Computing Machinery (ACM), Association for Information Systems (AIS) and Association of Information Technology Professionals (AITP, the new name for the DPMA). This curriculum consisted of a ten course core, much like the original DPMA '81 Model Curriculum, except that it incorporated support for e-commerce. The IS 2002 integrated traditional/client server computing with Web based client/server computing while all but eliminating the traditional main-frame computing [2].

In the 1990's object-oriented programming became popular. This naturally led to several architectures for programming with distributed objects [3]. These early architectures were based on Remote Procedure Calls and as a result had major problems with compatibility and security [4]. In 2000, many in the computer industry announced a strategy to convert their application architecture to Web services [5]. The movement to Web services and international, rather than enterprise, applications culminated in a new proposed curriculum by the ACM and AIS, the IS 2010 for Information Systems

Department of Computer Science,
The University of Texas at Tyler,
3900 University Blvd., Tyler, TX 75799.

ISBN 1-933510-99-4 /$15.00

[6] (cited with permission from Dr. Haekki Topi, Bentley University). The new curriculum has been designed to work well for both business-oriented programs, as well as for information systems programs in other departments as well. There is a small tightly-packed core of seven courses:

IS 2010.1 Foundations of Information Systems
IS 2010.2 Data and Information Management
IS 2010.3 Enterprise Architecture
IS 2010.4 IS Project Management
IS 2010.5 IT Infrastructure
IS 2010.6 Systems Analysis and Design, and
IS 2010.7 IS Strategy, Management and Acquisition

IS 2010.1 through IS 2010.6 cover most of the material of the IS 2002 core with an emphasis on Web services in IS 2010.3. One of the most interesting additions to the IS 2010 curriculum recommendations is the explicit addition of two security management courses:

IT Audit and Controls, and
IT Security and Risk Management

Another interesting feature of the curriculum is the introduction of a high-level final course, IS 2010.7, on the techniques that information science brings to bear on upper-level management decisions of today's international businesses.

The IS 2010 Information Systems curriculum has been submitted to the ACM and AIS for approval. When it, or something very similar, is approved most business-oriented computer science programs, including computer information systems programs, will need to adjust their curricula to reflect the changes taking place in business programming. However, before making changes it becomes necessary for the departments to first consider the impacts of the changes on courses approved for CNSS certifications.

II. The CNSS Certifications

Control of critical infrastructure by information systems has been an important recent development in most advanced societies [7]. However, it was also realized in the 1990's that such information systems were vulnerable to physical and cyber attacks. The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established by the National Security Directive 42 by President Bush [8] on July 5, 1990, for creating policies and procedures for national security systems. The NSTISSC was chaired by the Department of Defense and included several joint working groups. NSTISSC developed several instructions [9] for providing guidance and establishing technical criteria for specific national security systems issues – including the National Training Standard for Information Systems Security (INFOSEC) Professionals in June 1994 (NSTISSI-4011), and the National Training Standard for Systems Certifiers in December 2000 (NSTISSI-4015). In October 2001, the NSTISSC was redesignated as the Committee on National Security Systems (CNSS) [10]. CNSS developed further instructions including National Information Assurance Training Standard for Senior Systems Managers in June 2004 (CNSSI-4012) that superseded the NSTISSI-4012 developed in August 1997, National Information Assurance Training Standard for System Administrators (SA) in March 2004 (CNSSI-4013), Information Assurance Training Standard for Information Systems Security Officers in April 2004 (CNSSI-4014) that superseded NSTISSI-4014 developed in August 1997, and National Information Assurance Training Standard for Risk Analysts in November 2005 (CNSSI-4016).

Pursuant to President Clinton's Presidential Decision Directive (PDD) 63 [11], the National Security Agency (NSA) created the National IA Education and Training Programs (NIETP) which recognizes teaching institutions as National Centers of Academic Excellence in Information Assurance Education (CAEIAE) [12] provided the institutions satisfy nine stringent criteria [13]. Subsequent to the National Strategy to Secure Cyberspace in 2003 under President Bush, the CAEIAE was jointly sponsored by NSA and the Department of Homeland Security (DHS) [7]. The prerequisite for becoming a CAEIAE requires the institution to obtain certification under the Information Assurance Courseware Evaluation (IACE) program of NIETP [14]. The IACE program ensures that the academic standards of the institution meet those set by the Committee on National Security Systems (CNSS). For this purpose the candidate (for CAEIAE) institution should map its courses to one or more standards proposed by the CNSS: Information Systems Security Professionals (NSTISSI 4011), Senior Systems Managers (CNSSI 4012), System Administrators (CNSSI 4013), Information Systems Security Officers (CNSSI 4014), System Certifiers (NSTISSC 4015), and Risk Analyst (CNSSI 4016). It should be noted that the candidate institution should obtain certification for 4011 and one or more of the other certifications.

The CNSSI 4012 [15] establishes the minimum course content for training for Senior Systems Managers (SSM's) of national security systems. SSM's include the Chief Information Officer (CIO), Designated Approving Authority (DAA), and the Chief Technology Officer (CTO). SSM's responsibility includes analysis and judgment of requests for approval to operate information systems at a specified level of trust. This judgment should be based on a proper understanding of system architecture, system security measures, system operations

ISBN 1-933510-99-4 /$15.00

policy, system security management plan, legal and ethical considerations, and provisions for system operator and end user training. The Computer Information Systems (CIS) program is uniquely suited to training SSM's since graduates of this program are required to take courses in both Computer Science and College of Business: this trains the student for all competencies expected of an SSM. While CNSSI 4012 is a specific instruction issued by the CNSS, in this paper we will refer to CNSSI 4012 subsequently as CNSS 4012.

III. Security in IS curricula

The emphasis on security in the DPMA '81 curriculum was reflective of the general notions of security in the early mainframe days. Application security of COBOL programs was stressed in CIS 2 and CIS 3, mainframe operating systems security was briefly covered in CIS 3 as a part of file programming, network security was briefly covered in CIS-12 Data Communications, and security controls in the CIS-13 course on EDP Auditing. In the DPMA '86 curriculum [16], more time was spent on mainframe operating system and networking security in CIS-3. Mainframe applications security was still covered in CIS-2 and CIS-3, but the introduction of personal computer applications into the curriculum in CIS-2 was almost completely devoid of security concerns. The EDP auditing course was seen as the major place for security controls, but the new CIS-7 course on Data Center Management did an excellent job of integrating physical, operational and management security controls for mainframe computers.

In 1998, President Clinton declared that security was a priority for federal computer systems in the Presidential Decision Directive 63 [11]. This also declared that the quality computer security education was of importance to the federal government. By 2004, in response to the September 11th terrorist attacks, a number of CNSS instructions were published including the CNSS 4012 instruction for Senior Systems Administrators [15].This led to a number of information systems programs seeking CNSS 4012 certification from IACE. Thus by the publication of the IS 2002 curriculum, information science programs could legitimately attempt to embed a CNSS 4012 certification in an IS 2002 curriculum.

IS 2002 [17] had a 10 course core recommended and no recommended optional courses. Many of the core courses had a substantial security component. Specifically,

IS 2002.P0 Personal Productivity Software
In this course, instructors covered application security techniques used in developing macros for Off-The-Shelf programs.

IS 2002.1 Fundamentals of Information Systems
In this course about a tenth of the course is devoted to an overview of computer security and privacy.

IS 2002.2 E- Business Strategy, Architecture, and Design
This course includes coverage of network and internet security.

IS 2002.4 IT Hardware and System Software
This course includes coverage of operating systems security.

IS 2002.5 Programming, Data, File and Object Structures
This course includes coverage of application security.

IS 2002.6 Networks and Telecommunication
This course includes a thorough coverage of network, Internet and Web security.

IS 2002.8 Physical Design and Implementation with DBMS
This course includes a thorough coverage of database and file security.

The lack of optional courses in the IS 2002 curriculum resulted in schools developing and a variety of optional courses. Two popular optional courses were an EDP Auditing course that was much like that of the DPMA '86 curricula and a new course on Computer Security Management. The book [18] gives a typical description of this course which included security planning, risk analysis/management, security policy and certification/accreditation.

The IS 2010 curriculum includes a 7 course core. The first six classes in this curricula contain most of the material of the 10 course core of the IS 2002 curriculum. Thus the IS 2010 curricula will provide a complete introduction to information systems. In addition, the IS 2010 curriculum has two optional courses in security:

IT Audit and Controls, and
IT Security and Risk Management

Thus, it will be relatively easy for information systems programs to get a CNSS 4012 certification as the core curriculum and these two optional courses provide more than enough material.

From a practical point of view we believe that most information systems programs will opt to keep their current EDP Auditing and Computer Security Management courses, rather than replace them with the two recommended by the IS 2010. However, they may continue to offer separate computer hardware and networking courses, but this appears to be acceptable with the new curriculum's emphasis on a continuous improvement process. Another optional security course that would be a good addition to the IS 2010 curriculum would be a course on Web service security covering W*-Security as illustrated in [5].

ISBN 1-933510-99-4 /$15.00

Table 1. Relationship of CIS Courses at UT Tyler to IS 2010 and CNSSI-4012

Course Number	Course Name	IS 2002 Requirement	IS 2010 Requirement	Security Focus	Assignment Examples	CNSSI-4012 Functional Area
COSC 1310	Advanced Information Systems Software	IS2002.P0	IS2010.1	Introduction to Security	Class participation	None
COSC 2325	Foundations of Computer Information Science	IS2002.1	IS2010.1	Importance of Security in Information Systems	Class participation	None
COSC 2315	Computer Organization	IS2002.4	IS2010.5	Security related hardware issues	Class participation, homework	Satisfies NSTISSI-4011 Requirements
COSC 3310	Internet and Web Applications	IS2002.2	Elective Topic: Information Search and Retrieval	Authentication and Authorization	Class participation, project	None
COSC 3315	Social and Professional Issues in Computing	IS2002.3	Elective Topic: Social Informatics	Ethics in information systems development	Class participation, paper	None
COSC 3365	Programming with Data, File, and Object Structures	IS2002.5	IS2010.2	Security enhancing data structures	Class participation, project	None
COSC 3375	Analysis and Logical Design	IS2002.7	IS2010.6	Security considerations during requirements, design, and implementation	Paper; case studies; homework and exam questions	None
COSC 4309	Design of Modern Information Systems	IS2002.9	IS2010.3	User authentication and authorization; roles and privileges	Classwork example based on text; course project; exam questions	None
COSC 4325 (substituted by COSC 4360 Net-Centric Computing)	Data Communications and Computer Networks	IS2002.6	IS2010.5	Network security, risk assessment, business continuity, and intrusion prevention.	Class discussions, exam questions	Grant Final ATO, Review Accreditation, Verify Compliance, Allocate Resources, Multiple and Joint Accreditation, Assess Network Security (for COSC 4360)
COSC 4375	Information Systems Design Project	IS2002.10	IS2010.4	Security considerations during requirements, design, and implementation	Project documentation and implementation	None
COSC 4385	Database Design	IS2002.8	IS2010.2	Roles and privileges in databases	Class participation, homework, project	None
COSC 4362	Computer Security	-	Elective Topics: IT Audit and Controls	Major elements of computer security	Computer security lab; homework; team projects	All functional areas
COSC 4361	Computer Security Management	-	Elective Topic: IT Audit and Controls; IT Security and Risk Management	Risk assessment, vulnerability assessment, other elements of security management	Computer security lab; homework; team projects	All functional areas
?	(New Course)	-	IS2010.7: IS Strategy, Management, and Acquisition	-	-	Function 5: Ensure program managers define security in acquisitions

Legend: Underlined courses used for CNSSI compliance; ? indicates unknown number; - indicates unknown data

IV. MAPPING CNSS 4012 IN THE IS 2002 CURRICULA

CNSSI 4012 has elements in ten major functional areas each of which has additional sub-areas as described below.

Function 1 – Grant Final ATO (Approval To Operate):
This function includes responsibilities of SSM in information assurance (IA), issues related to accreditation, and process of obtaining ATO.

Function 2 – Review Accreditation:
This function covers threats to systems and their assessments, countermeasures, vulnerability analysis, and risk management.

Function 3 – Verify Compliance:
This function is concerned with laws related to IA and security, policy direction for information and personnel security, and security requirements.

ISBN 1-933510-99-4 /$15.00

Function 4 – Ensure Establishment of Security Controls:
This function is concerned with administration of security controls, access to security controls, procedures for incident handling and response, and planning for continuity of operations.
Function 5 – Ensure Program Managers Define Security in Acquisitions:
This function covers acquisitions processes as well as life cycle management for security.
Function 6 – Assign Responsibilities:
This function covers responsibility assignment for certification and accreditation, risk analysts, and information system security manager.
Function 7 – Define Criticality and Sensitivity:
This function covers aggregation and the liabilities associated with disclosure of classified information.
Function 8 – Allocate Resources:
This function is concerned with budget and resource allocation as well as business aspects of information security.
Function 9 – Multiple and Joint Accreditation:
This function explains the importance of the procedure to develop memoranda of understanding/agreement.
Function 10 – Assess Network Security:
This function discusses network connectivity, emissions security, and security related to wireless technology.

When an institution maps its courses it has been recommended that they use a minimum set of courses for IACE approval that together satisfy all elements of all the functional areas. At UT Tyler we mapped three courses to all elements of CNSS 4012: COSC4360 Net-Centric Computing, COSC4361 Computer Security Management, and COSC4362 Computer Security. These courses have been offered once each academic year for the past five years and the average enrollment has been 15 students per class.

We started our mapping process in the summer of 2008 and completed it by the deadline of January 15, 2009. We needed to enter course-wise mapping for about 300 elements of the CNSS 4012 and spent several hours on the IACE website for this process. Incidentally these three courses also mapped to several elements of NSTISSI-4011 and by including one more course COSC2315 Computer Organization we completely mapped all elements of 4011 as well. We received approval from IACE in April 2009 for both 4011 and 4012 certifications along with very positive feedback from the reviewers. We will have our first batch of students receiving both these certifications graduating from our programs this semester (Spring 2010).

Now let's consider how these courses map to the IS 2002 curriculum requirements. The courses offered in our CIS program along with their IS 2002 equivalents are shown in Table 1 – underlined courses in Table 1 have been used for mapping to CNSS 4012 and NSTISSI-4011 standards. As can be seen from that table, while COSC2315 (used for 4011) maps to the IS 2002.4 requirements, COSC4325 Data Communications and Computer Networks maps to the IS 2002.6 requirements. However, courses COSC4361 and COSC4362 are not mandated by IS 2002 curriculum but are required to satisfy CNSS 4012 requirements. Since we mapped COSC4360 (offered as part of the Computer Science curriculum) to CNSS 4012, we approved substitution of COSC4360 for COSC4325 for all CIS students interested in CNSS 4012 certification. Therefore, it may be concluded that strict adherence to IS 2002 requirements will not enable an institution to satisfy CNSS 4012 requirements. It should be noted that Table 1 only lists those courses offered by the CIS program in the Department of Computer Science at UT Tyler; students also take several (at least four) courses in the College of Business to complete their graduation requirements.

V. Mapping CNSS 4012 in the IS 2010 curricula

We now consider the effect of the proposed IS 2010 curricula on CNSS 4012 requirements. There are seven core courses in IS 2010 [6, 20] IS 2010.1 through IS 2010.7. However, in IS 2010 there is only one core course on IT Infrastructure: IS 2010.5 and not two as in IS 2002 (IS 2002.4 and IS 2002.6). While it may be tempting to drop either COSC2315 or COSC4360 to conform to IS 2010, in order to be CNSS 4012 we need to offer both these courses (we need to keep in mind that compliance with CNSS 4012 first requires compliance with NSTISSI-4011, and therefore we need COSC2315 which helps us be in compliance with the latter).

Moreover, IS 2010 explicitly recognizes the need for security courses in the curriculum by adding two optional courses in security: IT Audit and Controls, and IT Security and Risk Management. The focus of IT Audit and Controls course is to develop an understanding of information controls, the types of controls and their impact on the organization, and how to manage and audit them. The IT Security and Risk Management course addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational IT Security and Risk Management. Our COSC4361 and COSC4362 courses meet the requirements for both these courses in IS 2010 and, therefore, compliance of our program with IS 2010 requirements will also imply compliance with CNSS 4012 requirements, as illustrated in Table 1.

However, our curriculum currently does have an equivalent for IS 2010.7 and this would necessitate introducing a new course to satisfy this requirement. An

ISBN 1-933510-99-4 /$15.00

additional advantage of this new course will be that it can satisfy Function 5 (Ensure Program Managers Define Security in Acquisitions) of CNSS 4012 and can be added to the basket of courses for complying with CNSS 4012 requirements – however, this will require IACE approval. However, we are currently proceeding further on our path to become a CAEIAE by satisfying the criteria [13] set by NIETP.

In addition to meeting IS 2010 requirements, we plan to obtain Accreditation Board for Engineering and Technology (ABET) [19] accreditation for our improved CIS curriculum. For this purpose we plan to retain most of the courses indicated in Table 1 and add the new course for satisfying IS 2010.7 requirements. However, since we need to show continuous improvement cycles for ABET accreditation we estimate it will take our program another couple of years to be ready for accreditation.

VI. Observations

From our analysis of IS 2002 and IS 2010 curricula we can conclude the following:

1. Courses currently satisfying IS 2002 curricula are by themselves not sufficient to satisfy IS 2010 curricula requirements.
2. New courses will be needed for current programs in computer information systems to satisfy IS 2010 curricula requirements.
3. Courses currently meeting IS 2002 curricula are by themselves not sufficient to satisfy CNSS 4012 requirements.
4. However, the courses added to IS 2002 curricula to satisfy CNSS 4012 requirements will help considerably in satisfying most of the requirements for IS 2010 curricula.
5. Additional courses added to meet IS 2010 requirements may necessitate redistribution of material for CNSS 4012 certification and this may require approval of the new additions by IACE.
6. At University of Texas at Tyler we believe that only one more course may need to be added to our current set of courses to satisfy both IS 2010 and CNSS 4012 – this course will be equivalent to IS 2010.7 and may need to be included in the set of courses for obtaining CNSS 4012 certification (which means, it may need IACE approval).
7. The most important point is that it is possible to meet the IS 2010 curriculum requirements and the CNSS 4012 certification requirements at the same time – this should encourage information systems programs to seek CNSS accreditation for their courses.

VII. Summary

Over time several model curricula have been developed for information systems education. It started in 1981 with the DPMA (Data Processing Management Association) model curriculum, which evolved through 1986 DPMA model curriculum into the IS 2002 model curriculum. IS 2002 has served as the standard for several Computer Information Systems (CIS) programs in the United States including at University of Texas at Tyler. CIS programs based on IS 2002 have also need to comply with the federal government requirements for imparting security instruction for Senior Systems Managers employed by the federal government, chiefly the CNSS 4012 requirements. The CIS program at UT Tyler evolved to meet the CNSS 4012 standard and received approval from National Security Agency's Information Assurance Courseware Evaluation (IACE) program in 2009. However, in November 2009, the IS 2010 draft curriculum was proposed and it mandates certain changes to the CIS curriculum. We observed that IS 2010 streamlines CIS curriculum and brings it in line with modern trends in information technology. We also observed that while adopting IS 2010 model will require addition of at least one new course, it will not significantly affect our compliance with CNSS 4012 standard.

VIII. Acknowledgement

We thank the anonymous reviewers of the earlier version of this paper for their insightful suggestions and comments which helped us improve the final version.

IX. References

[1] Data Processing Management Association, "CIS '81, The DPMA Model Curriculum for Undergraduate Computer Information Systems," *DPMA*, 1981.
[2] Whitson G. "From Advanced Cobol to Data, File and Object Structures," The Journal of Computing Sciences in Colleges 22(5): 39-45, 2007.
[3] History Making Components, IBM Developworks, http://www.ibm.com/developerworks/webservices/library/co-tmline/, retrieved March 10, 2010.
[4] Whitson G. "Distributed Objects: A New programming Paradigm," The Journal of Computing Sciences in Colleges 12(4): 11-25, 2007.
[5] Whitson G. "Security for Service Oriented Architectures," Journal of Computing Sciences in Colleges 23(4): 8-9, 2008.
[6] IS 2010: Curriculum Guidelines for Undergraduate Programs in Information Systems, November 23, 2009, retrieved from http://blogsandwikis.bentley.edu/iscurriculum/index.php/Main_Page on March 10, 2010.

ISBN 1-933510-99-4 /$15.00

[7] Geoghegan S. J. "The Development of an Information Assurance Program", Journal of Computing Sciences in Colleges 23(4): 116-123, 2008.
[8] http://cryptome.org/nstissc.htm, retrieved on March 13, 2010.
[9] http://www.cnss.gov/instructions.html retrieved on March 13, 2010.
[10] http://www.cnss.gov/history.html, retrieved on March 13, 2010.
[11] Presidential Decision Directive/NSC-63, 5/22/1998, www.fas.org/irp/offdocs/pdd/pdd-63.htm, retrieved on March 13, 2010.
[12] http://www.nsa.gov/ia/academic_outreach/index.shtml retrieved on March 13, 2010.
[13] http://www.nsa.gov/ia/academic_outreach/nat_cae/cae_iae_program_criteria.shtml retrieved on March 13, 2010.
[14] http://www.nsa.gov/ia/academic_outreach/iace_program/index.shtml retrieved on March 13, 2010.
[15] CNSS Instruction No. 4012 National Information Assurance Training Standard for Senior System Managers issued in June 2004.
[16] Data Processing Management Association, "CIS '86, The DPMA Model Curriculum for Undergraduate Computer Information Systems," *DPMA*, 1986.
[17] ACM/AIS/AITP Joint Curriculum Task Force, "IS '2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems," ACM, AIS and AITP (formerly DPMA).
[18] Whitman, Michael E., and Mattord, Herbert J., Principles of Information Security, Second Edition, Florence, KY: Thompson Course Technology, 2005.
[19] http://www.abet.org retrieved on March 13, 2010.
[20] Topi, H., "IS 2010 Is Ready and Available for Your Use!", ACM Inroads, March 2010, Vol. 1, No. 1, pp. 16 – 17.

ISBN 1-933510-99-4 /$15.00