

Developing IA Courses Based on the CNSS 4016 Standard

George Bailey and Melissa J. Dark, PhD
Purdue University
baileyga@purdue.edu, dark@purdue.edu

Abstract-This paper describes a set of two courses for teaching students Information Security Risk Analysis and Risk Management. This paper discusses how the courses map to the CNSS (Committee on National Security Systems) 4016 Information Security Risk Analyst standard and will serve as a model for institutions and faculty wishing to develop courseware that aligns to the most recent CNSS standard. In addition, this paper discusses the specific instructional methods and assessment that are used in the courses with the intent of providing others with ideas about teaching risk analysis.

1. INTRODUCTION

Many risk analysis (RA) courses are based on industry information security standards, such as ISO17799, CoBit 4.0, the NIST SP-800 series, etc. These standards are strong in recommending suitable organizational policies, procedures, and security best practices. However, these standards do not outline the necessary skills needed by professionals performing risk analysis and risk management duties. The creation of CNSS training standards should help in solving this problem by presenting the recommended skill sets that IA professionals should possess in order to perform RA duties. Currently there are few information assurance courses that map to the CNSS 4016 standard. The purpose of this paper is to present a detailed example of such a mapping. This paper has four sections. First, we provide background information on the Committee on National Security Systems (CNSS). Second, we describe the CNSS 4016 standard in more detail. Next, we introduce the course that was developed prior to the CNSS 4016 standard and describe how this course maps to CNSS 4016. We continue by discussing how gaps were identified and used to design a second course in a set of two that will strive to meet the CNSS 4016 standard. Last, we present how the new course was developed to address some of those gaps in the previous course.

2. BACKGROUND

On October 16, 2001, President Bush redesignated the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems (CNSS) by signing Executive Order 13231 on Critical Infrastructure Protection [1]. The CNSS provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operation procedures, and guidance for the security of national security systems [2]. National security systems are information systems operated by the U.S. Government, its contractors or agents that contain classified information or that involve:

1. intelligence activities;
2. cryptographic activities related to national security;
3. command and control of military forces;
4. equipment that is an integral part of a weapon or weapons system(s); or
5. Are critical to the direct fulfillment of military or intelligence missions (not including routine administrative and business applications).

The CNSS is supported by two subcommittees, the Subcommittee on Telecommunications Security (STS) and the Subcommittee on Information Systems Security (SISS). These subcommittees share information and coordinate recommendations concerning implementation of protective measures. They develop and issue guidelines, instructions, advisory memoranda, technical bulletins, and incident reports. The subcommittees are comprised of representatives from the 20 member organizations on the committee [2].

The instructions (standards), created by the CNSS are binding upon all U.S. Government departments and agencies [3]. These standards provide guidance and establish technical criteria for specific national security systems issues. These standards include technical or implementation guidelines, restrictions, doctrines, and procedures applicable to information assurance. Currently there are 11 such standards available addressing many areas of information assurance training. The latest standard is CNSS 4016 – National Information Assurance

Training Standard for Risk Analysts, dated November 2005 [4]. This document provides minimum training standards for those performing risk analyst functions for national security systems. It also offers guidelines for those performing risk analyst functions for unclassified systems. This is the most comprehensive training standard on risk analysis and risk management to date.

3. A DETAILED LOOK AT CNSS4016

The CNSS 4016 standard consists of 9 functional areas presenting a range of skills required of persons performing risk analysts functions. Each functional area lists skills as entry, intermediate, or advanced level competencies. The nine functional areas of the CNSS 4016 standard are [4]:

1. Information Life Cycle Activities
2. Countermeasures, Identification, Implementation, and Assessments
3. Certification and Accreditation
4. Synthesis of Analysis
5. Testing and Evaluation
6. Threat and Adversary Analysis
7. Mission and Assets Management
8. Vulnerabilities and Attack Avenues Analysis
9. Training and Awareness

4. THE EXISTING COURSE

The course uses existing quantitative and qualitative risk assessment methodologies [5], [6], [7]. Students in the course are required to conduct a comprehensive information security risk assessment using risk assessment models/methodologies to assess information security practices as they relate to technology, policy, and people. In this class students work in teams to provide information security risk assessment consultation to a non-profit client. Depending upon course enrollments, there are 4-6 teams with 3-5 students per team. Each team is assigned to a client with larger teams assigned to larger clients in an attempt to allocate resources proportionately.

4.1 Course Description and Objectives

The C&IT 528 course description and objectives are described below. They have been paraphrased for the purposes of this paper.

Students spend the first 7 weeks of the class learning through more traditional methods, i.e., lecture and reading. However, for the next 7 weeks of the class, students are assigned to a team tasked with performing an information security risk assessment for a client, which will be a K12 school corporation in the west central area of Indiana.

This service learning course intends to provide an education experience:

- whereby students learn and develop through active participation in thoughtfully organized service experiences that meet actual community needs, that are integrated into the students' academic curriculum or provide structured time for reflection, and that enhance what is taught in school by extending student learning beyond the classroom and into the community.
- that increases the civic responsibility and citizenship of students in the course; this occurs by exposing students to societal inadequacies where they can use the community service experience as a foundation for learning 1) about oneself, 2) the academic discipline, 3) real world skills and techniques, and 4) how the discipline, skills and techniques intersect with the social world around us.
- that joins theory and practice, i.e., students experience the relevance of the subject to the real world. Students in service learning courses are empowered to make a difference with the skills they are learning in an environment where there is a need; furthermore, the learning experience and student learning outcomes are usually richer when there is a distinct and known need for the service.

4.2 Course Objectives

After completing the course, students were able to:

- Conduct an information security risk assessment.
- Perform asset identification and classification
- Perform threat identification
- Perform vulnerability identification
- Perform control analysis
- Perform likelihood determination
- Conduct impact analysis
- Conduct risk determination
- Identify control recommendations
- Document results
- Identify pertinent standards and regulations and their relevance to information security management.
- Describe legal and public relations implications of security and privacy issues.

4.3 Identifying the Gap

The Information Security Risk Assessment class existed before the CNSS 4016 Information Security Risk Analyst standard was released. Therefore, when the standard was released our first step was to identify the elements of the standard that the existing course already met. By understanding the elements that we already met, we could focus our effort on creating a second course that addressed gaps to suffice 4016 certification requirements.

Figure one shows the portion of 4016 that is covered in C&IT 528. The x axis includes the 9 functional areas of CNSS 4016, which are: 1) Life cycle duties, 2) Countermeasures Identification, Implementation and Assessments, 3) Certification and Accreditation, Synthesis of Analysis, 5) Testing and Evaluation, 6) Threat and Adversary Analysis, 7) Mission and Assets Assessment, 8) Vulnerabilities and Attack Avenues Analysis, and 9) Training and Awareness.

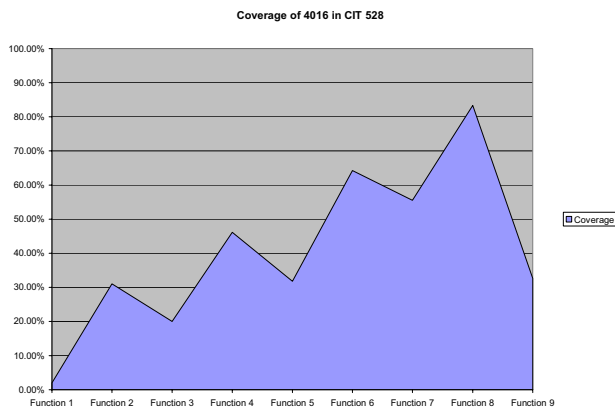


Figure 1: CNSS 4016 Covered in C&IT 528 by Functional Area

Based on the mapping done, C&IT 528 clearly addresses much more of functions 8, 7, 6, and 4 than of functions 9, 5, 2, 3 and 1. Interestingly, when the standard is analyzed for coverage of entry, intermediate, and advanced level knowledge in addition to functional area, C&IT 528 covers 50.79% of the entry level competencies addressed in the standard; 21.49% of the intermediate level competencies; and 22.22% of the advanced level competencies as shown in Figure 2.

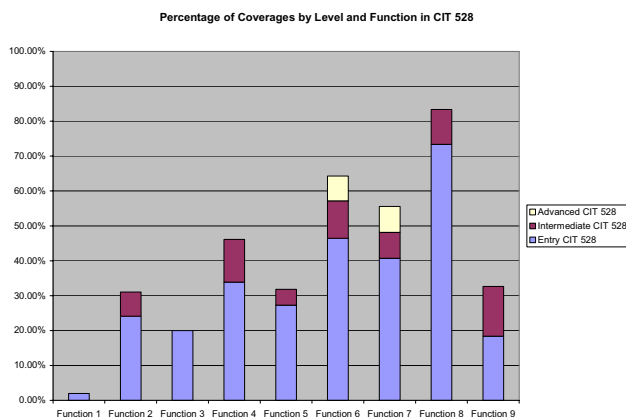


Figure 2: C&IT 528's Coverage by Competency Level

The reason that we point this out is that often mapping to a standard such as CNSS is not an easy, one to one

correlation. It is not easy to teach only certain functional areas as evidenced by the spread in C&IT 528 across the 9 functional areas. Nor is it easy, or necessarily instructionally effective to map only to a level, i.e., entry, intermediate or advanced. As educators, our job is not necessarily to map to a standard, such as CNSS 4016. Our job is to prepare curricula that we believe will prepare qualified graduates and often the way to deliver these curricula does not show a direct correlation with job standards. We struggled with this as we tried to model what we are already covering in order to know what to cover in the second course.

Once we had a clear picture of what C&IT 528 covered, we identified what we wanted the second course to address, which is not the entire remainder of the CNSS 4016 standard.

5. SECOND COURSE

The C&IT 529 course description and objectives are described below. They have been paraphrased for the purposes of this paper.

5.1 Course Description

This course is a continuation of the C&IT 528 service learning course, where students will develop risk management strategies for their host organization. Students will spend 15 weeks learning about risk mitigation strategies from a variety of reading, writing, research and presentation activities. C&IT 528 is generally made up of graduate students from interdisciplinary programs. It is likely that not all students from the preceding C&IT 528 course will choose to continue on to the next course. Because of this, we decided that it would be best if students work independently with an occasional group activity in this second course. The semester's work will be combined into a risk management strategy report based on the learning outcomes from both courses. The risk management strategy report will contain recommended countermeasures along with an estimated cost-benefit analysis, framework for the development of a certification and accreditation program along with, frameworks for the creation of an incident response and training/awareness programs.

5.2 Course Objectives

After completing the course, students will be able to:

- Identify stages of a system life cycle, relate role of security management at each stage
- Apply risk management methodologies to the life cycle of information systems

- Conduct an information criticality analysis
- Recommend security requirements to best protect information systems
- Determine residual risk by applying risk management methodologies to the evaluation of threats, vulnerabilities and countermeasures
- Analyze effectiveness of countermeasures to maximize risk mitigation
- Perform a cost/benefit analysis of IA countermeasures
- Document activities related to the IA certification and accreditation of information systems
- Identify policies, procedures, and methodologies to be included in an IA training and awareness program
- Recommend requirements for an organizational incident response framework.
- Identify pertinent standards and regulations and their relevance to information security management

5.3 Closing the Gap

The CNSS 4016 standard was released before the second course was created. As alluded to earlier, it was our goal to try to conduct a one to one mapping from the standard to the two courses, but we quickly discovered while creating the second course that a one to one correlation was not practical. Due to time constraints, instructional methods, and lack of prerequisite student knowledge; covering 100% of the standard was not feasible in two courses.

Figure 3 shows the total CNSS 4016 coverage provided in the second course across all three competency levels. It was decided that it would be best to focus our efforts and cover as many of the entry level competencies as possible. This is for practical reasons; simply put, for institutions wishing to map to the standard, they have to select a level (beginning, intermediate or advanced) to map to. We decided to cover some of the intermediate and advanced level competencies in the second course where it made sense to do so to improve student learning, enhance group activities and foster classroom discussions. Figure five shows the combined CNSS 4016 coverage from both C&IT 528 and C&IT 529. As shown in the graph, 100% coverage of all nine functional areas was not possible.

The second course covers 31.4% of the entry level, 18.9% of the intermediate level, and 13.6% of the advanced level competencies. Figure 4 shows C&IT 529's break down by competency level covered by each functional area.

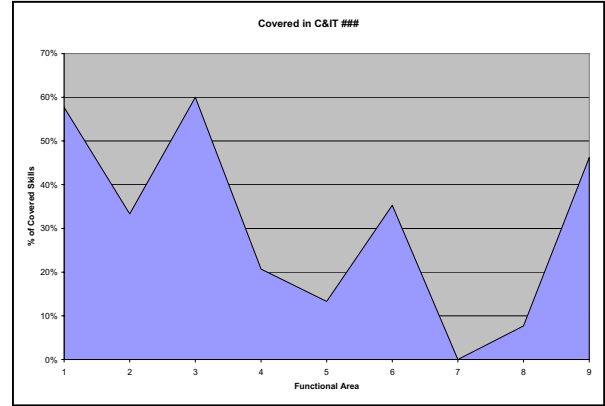


Figure 3: CNSS 4016 Coverage in C&IT 529 by Functional Area

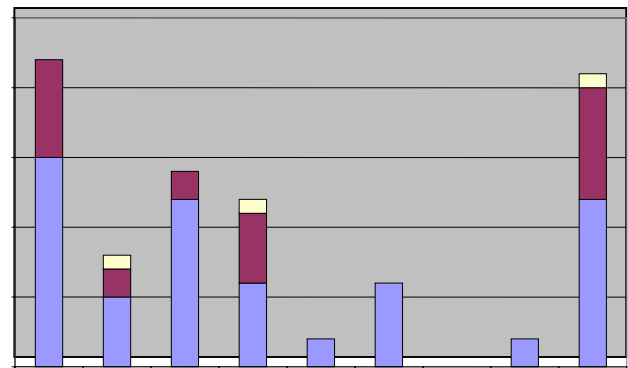


Figure 4: C&IT 529's Coverage by Competency Level

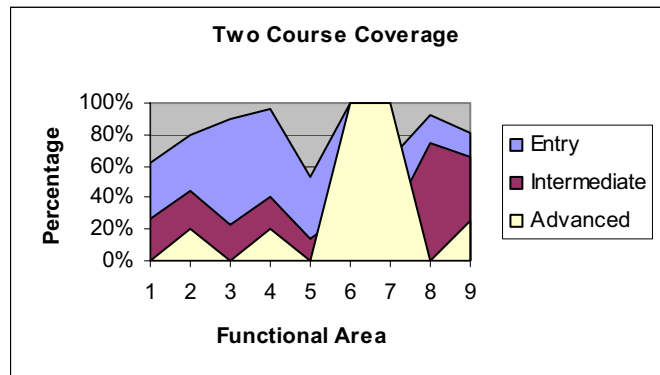


Figure 5: Combined Coverage

Besides trying to cover the entire 4016 standard in two courses, the other significant problem that we had to address was creating homework exercises that coincided with the lecture material. For an experienced IA instructor, creating lecture material to cover the required topics may not be difficult. However, creating exercises that are worth while to students and that provide a sense “real world” value as we had in the first course is not so easy. Being a graduate course, there is a great deal of

writing required of the students. We tried to make the assignments build on one another. For example, students were required to take the final output of the previous course and condense it into an executive summary. This summary is the foundation of the risk management report that is developed over the course of the semester. Each individual writing assignment is an actual section of the risk management report that is the final deliverable of the course.

6. CONCLUSION

Using standards such as those created by the CNSS organization can be helpful to faculty teaching information assurance courses to determine what topics need be covered to prepare students to enter the IA field as practitioners. However, because the standards don't lend themselves to a one to one correlation of required skill set to teachable task as we experienced, they should only be used a guide. IA faculty wishing to use the CNSS standards to assist in curriculum development will have to incorporate more hands on activities and problem based learning to cover the skill sets that are not acquired from a text book and traditional lecture.

REFERENCES

- [1] Bush, G. W. (2001, October 16, 2001). *Executive Order on Critical Infrastructure Protection*. Retrieved April 1, 2006, from <http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html>
- [2] CNSS. (2001). *CNSS Web Page*. Retrieved January 10, 2006, from <http://www.cnss.gov/>
- [3] NSTISS. (1992). *National Training Program For Information Systems Security (INFOSEC) Professionals* (No. NSTISSD-501).
- [4] CNSS. (2005). *National Information Assurance Training Standard For Risk Analysts* (No. CNSSI-4016).
- [5] NIST (2001). *Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology*. Available at: <http://csrc.nist.gov/publications/nistpubs/index.html>
- [6] Peltier, T. (2001). *Information security risk analysis*. Auerbach: Boca Raton, FL.
- [7] Tipton, H. & Krause, M. (Eds.). (2000). *Information security management handbook, 4th edition*. Auerbach: Boca Raton, FL.