

Developing IA Courses Based on CNSS 4016

George Bailey
Purdue University

Introduction

- Committee on National Security Systems (CNSS)
- CNSS 4016 – Risk Analyst Training Standard
- Course #1: C&IT 528 - Risk Analysis
- Closing the Gap
- Course #2: C&IT 529 - Risk Management
- What's Next

Background

- Committee on National Security Systems (CNSS), formerly National Security Telecommunications and Information Systems Security Committee (NSTISSC)
- 20+ members from U.S. Government Departments and Agencies that are given voting privileges for all CNSS activities
- 11 IA standards covering a variety of training and certification areas
- 11 IA policies that address national security systems issues from a broad perspective and are binding upon all U.S. Government departments and agencies
- 5 IA directives that provide details for achieving CNSS policies

Looking Closer at CNSS 4016

Information Assurance Training Standard For Risk Analysts

<http://www.cnss.gov/>

- Newest standard, released November 2005
- 330 Total Skills
 - 191 – Entry Level
 - 121 – Intermediate Level
 - 18 – Advanced Level
- 9 Categories
 - Information Life Cycle Activities
 - Countermeasures, Identification, Implementation, and Assessments
 - Certification and Accreditation
 - Synthesis of Analysis
 - Testing and Evaluation
 - Threat and Adversary Analysis
 - Mission and Assets Management
 - Vulnerabilities and Attack Avenues Analysis
 - Training and Awareness

Pros & Cons

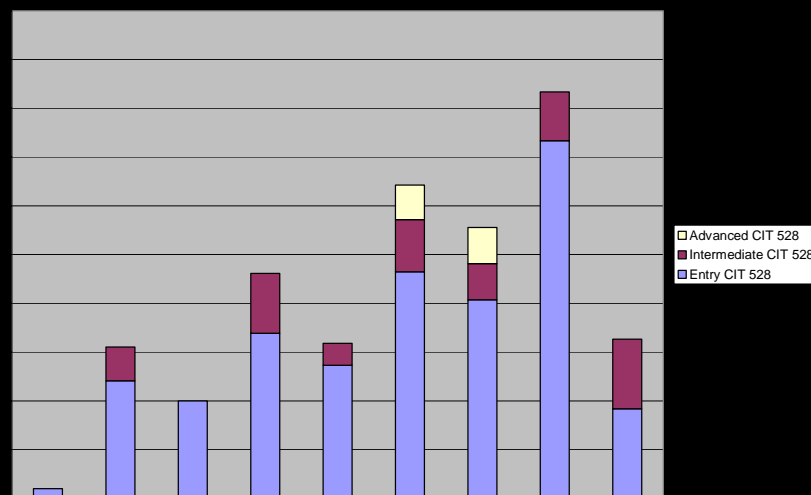
- Detailed listing of required skill sets
- Covering many different infosec domains
- Broken down into three different skill levels

- Some skills overlap domains at different skill level
- Scope of skill levels not clearly defined
- Difficult standard to map to training materials
- No metrics for determining skill set level

C&IT 528

Risk Analysis

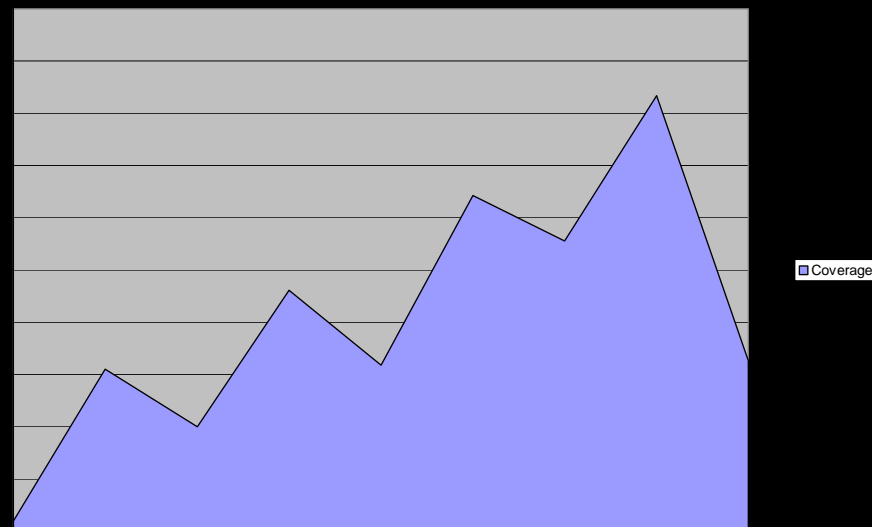
- Service learning course
 - 7 weeks traditional learning
 - Lecture, guest speakers, reading, writing
 - Process, People, Technology
 - 7 weeks on-site with K-12 organization
 - Team lead risk assessment
 - Active learning
 - Problem based learning
 - Problem / Vulnerability Research
 - > 50% CNSS 4016 coverage



C&IT 528

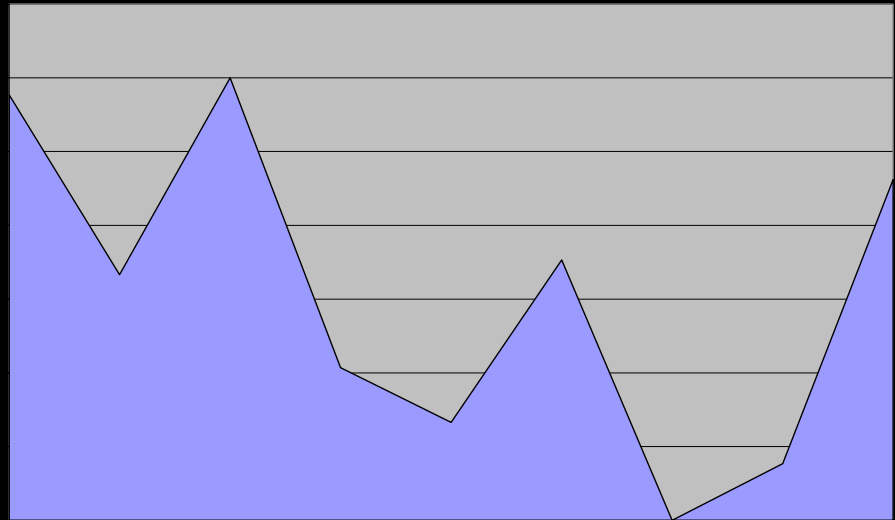
Course Objectives

- **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**



Closing the Gap

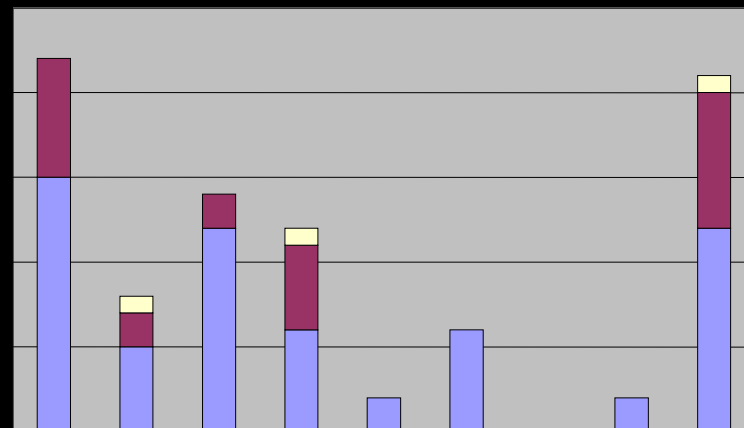
- Standard released after C&IT 528
- Coverage determined by course deliverables – reading, writing, presentations
- CNSS 4016 too broad to cover in two courses
- One-to-one mapping not practical
- Goal – Cover 100% of Entry level skills



C&IT 529

Risk Management

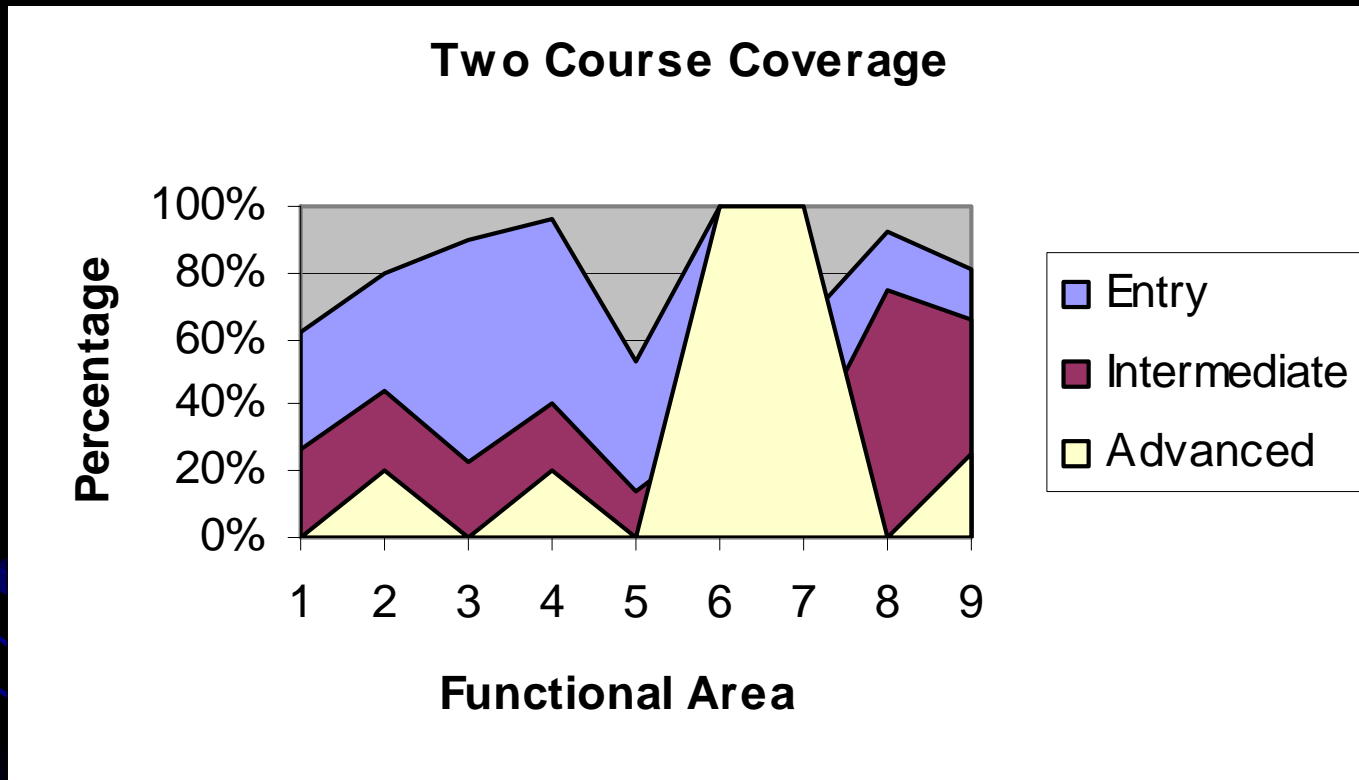
- Continuation of C&IT 528
 - Traditional learning environment
- Closely mapped to CNSS 4016
 - Course objectives & learning outcomes inspired by CNSS 4016
- > 50% CNSS 4016 coverage



C&IT 529: Course Objectives

- **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.**

Total Coverage



What's next

- Expand on the CNSS 4016 offerings
 - Fill the gaps by diversifying course offerings
 - Get creative with problem based learning
 - Undergraduate & graduate research opportunities
- Build course modules for distance IA education
- Share course materials with other colleges & universities

Questions



Contact

George Bailey

Purdue University

West Lafayette, Indiana

baileyga@purdue.edu,

gbailey@ivytech.edu

(317) 921-4526