**IUPUI**
**Academic Policies and Procedures Committee**
**Minutes**
**Friday 5/7/04**
**1:00—3:00**

**NOTE ROOM LOCATION—UL 1126**

**Minutes**
- 4/2/04 minutes were accepted.

**Announcements**
- Items from the Chair
  - Update on Financial Aid Award Notifications
    - Financial Aid Notification letters have been mailed to new Medical, Law, and Dental students and new freshman.
    - New Freshmen were package as full time (12 credits). Awards will be adjusted after the students register.
  - Registrar interviews
    - The search and screen committee has invited candidates for the Registrar position to campus for interviews.
    - APPC members are invited to the presentations. Individuals interested on going to dinner with a candidate should contact Nasser Paydar or Mark Grove.

**Academic Affairs Committee Report** *Betty Jones, Chair*

No report

**Items for Review, Discussion, or Action**
- Update on SIS
  - The schedule of classes for spring is currently being built. Unfortunately it can not be masked from view as it is being constructed. Be aware of this limitation.
  - The degree audit for the pilot programs will be available in the near future. A communication will be sent to advisors indicating that the degree audit process should not be used widely at this time since it remains in the pilot mode.
- Parents/spouses contacting offices for information about students—*Joe Kuczkowski, Mark Grove, Tom Gannon*
  - Information on the regulations is available on the Registrar's website http://registrar.iupui.edu/ferpa/
  - The most prudent step to take is simply to refer callers to the Office of the Registrar. If appropriate forms are completed by a parent, the Registrar will notify the school and faculty (as appropriate) that they are free to talk with parents, but faculty are not required to discuss performance or attendance in a class. The Registrar's Office will emphasize that attendance isn't taken in the same way it was in high school. Spouses may not have access to student information without the specific approval of the student.
  - In cases where the student accompanies the parent or spouse/partner, there is an implied consent from the student to share information.
- Certificate in Network Security—*Ken Rennels*
  - The proposal for the Certificate in Network Security was reviewed. The report from the reviewers is appended to the minutes.

- After discussion of the proposal, the members of the APPC agree that the Certificate was an appropriate addition for IUPUI.

- Policies on retaining student work—*Rick Ward*
  - The policy in School of Liberal Arts is to retain documents for one year unless specified in the course syllabus.
  - Faculty are being encouraged to specify a defined period that work will be available for the student to retrieve (e.g. 2 weeks after the posting of final grades)
  - The development of the electronic portfolio may decrease the volume of papers that have to be dealt with.
  - A draft set of record retention guidelines will be available this summer as a result of work by Mike Donahue and Mark Grove with Steve Towne of University Archives. This Website is intended to provide guidance to the schools and faculty on how long to keep specific documents.
- Policies on retaining student evaluations of faculty—*Rick Ward*
  - The Faculty Affairs Committee position is that evaluations belong to the faculty member so the original documents should be provided the faculty member
  - The department will keep a copy of the summary information
- Doubling Task force on Teaching and Learning
  - Bill Kulsrud attended the meeting on behalf of Scott Evenbeck
  - Copies of the final report were distributed at the meeting
  - Concerns with areas of the report were discussed.
- Limitation of the transfer of courses from 2 year institutions to 100 or 200 level courses
  - UFC policy states that courses from 2 year institutions can only transfer as equivalent to 100 and 200 level courses. This poses a problem at IUPUI since several courses typically taught at 2 year institutions (such as Abnormal Psychology) are listed as 300 level courses at IUPUI.
  - Both Psychology and SPEA have identified IVY Tech courses in which the faculty have determined that the course is equivalent to a 300 level IUPUI course. They support transferring the coursework as equivalent.
  - To accommodate the UFC policy, a 'pseudo' course at the 200 level has been created so that the transfer can occur.
  - APPC discussed the pros and cons of seeking an amendment to the UFC policy to permit the transfer of courses from a 2 year institution to a 300 level course with the specific approval of the faculty of the unit.
  - Discussion will continue next fall.

**Future Agenda Items**

- Adult Learner Focused Institution Coalition (ALFI)—*Amanda Zimmerman*

**Meeting Dates and Locations**

There are no regularly scheduled APPC meetings during the summer. Meetings will be convened on an as needed basis.

**Indiana University**

**Request for a Certificate Program**

**Campus**: Indiana University Purdue University Indianapolis

**Proposed Title of Certificate Program**: Network Security Certificate

**Projected Date of Implementation**: Spring 2004

**1. Why is the certificate needed (Rationale)**

> "As you may be aware, there is a critical shortage of skilled information assurance professionals in the workforce - this is true across several industry sectors including government, education, telecommunications, finance, health care, energy, and so on. This problem is further exaggerated by the fact that we do not have enough colleges and universities educating professionals to meet the workforce need."

This statement by Dr. Melissa Dark is indicative of the state of Information Assurance (IA) and security professionals in today's marketplace (Dark, n.d.). Several initiatives have been implemented to address this shortage, from educating faculty to teach Information Assurance to developing new IA programs for students. (Spanninger, 2001) In particular, the National Security Agency (NSA) has funded several programs in Information Assurance and Security under the Information Assurance Awareness, Training, and Education Partnership (IAATREP) Program. The IAATREP program was funded with the long-term goal of improving the national state of Information Assurance.

The short-term outcome of the IAATREP program is to provide quality education and training in Information Assurance to educators. Increasing the number of educators well versed in IA will, in turn, help to increase the number of qualified students entering the IA field. This will help increase the number of IA professionals qualified to help safeguard our nation's increasingly vulnerable information infrastructure. (Overview of the NSA IAATREP Program, n.d.)

To help meet this need, the Computer and Information Technology (CIT) Department at Indiana University Purdue University Indianapolis is developing a Network Security Certificate (NSC) to provide Information Assurance education and training to students and professionals. Completion of the NSC will prepare participants for jobs in Information Assurance and network security. As a first step in developing this certificate Connie Justice, the networking track coordinator, completed the Information Assurance Education Graduate Certificate (n.d.) offered by the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. This 11-credit hour certificate program, funded by IAATREP, prepares faculty to teach and create information assurance and security programs.

Courses for this certificate were developed by mapping course content to National Security Telecommunications and Information Systems Security Instruction (NSTISSI) standards set by the National Security Telecommunications and Information Systems Security Committee

(NSTISSC). By doing so, the program can receive formal certification from the National INFOSEC Education and Training Program segment of the NSA. Certification by the NSA allows our institution to issue Information Systems Security (INFOSEC) certificates to our students.

**2. List the major topics or curriculum of the certificate.**

The Network Security Certificate program addresses the need to educate students and professionals in Information Assurance. It is designed so that it can be completed within one calendar year. This allows professionals working in security to complete the certificate in a timely manner. It is also designed so that all courses in the certificate can be applied directly to a Bachelor's degree program in our department, so that degree-seeking students can also earn this certificate.

The Network Security Certificate consists of six 3-credit hour courses for a total of 18 credit hours. A brief description (bulletin descriptions) of each of these courses is shown below. Fuller information is provided in the attached New Course Requests. Three of these courses (CIT 303, CIT 415 and CIT 406) are currently being taught by our department, the last two under our variable 499 title. CIT 420 and CIT 431 are new courses which are under development.

Prerequisite knowledge for the certificate can be met in many ways:

- An Associate's degree in a technology area with knowledge of basic data communications concepts, discrete math, and probability or statistics, which would be met by the A.S. in CIT. For students with an A.S. in other subjects, this requirement can be met by completion of CIT 307 Data Communications, CIT 120 and CIT 220, or equivalent coursework.
- Professional certification in network and system administration such as a Microsoft Certified System Engineer
- Three or more years of experience in network and systems administration.

**CIT 303 Communication Security and Network Controls**
Prerequisite: CIT 307 or ECET 284 or consent of Course Coordinator

This course will provide students with an overview of the field of Information Security and Assurance. Students will explore current encryption, hardware, software and managerial controls needed to operate networks and computer systems in a safe and secure manner.

**CIT 406 Advanced Network Security**
Prerequisite: CIT 303

This course provides students with the in-depth study and practice of advanced concepts in applied systems and networking security, including security policies, access controls, IP security, authentication mechanisms and intrusion detection and protection.

**CIT 415 Advanced Network Administration**
Prerequisite: CIT 317 or CIT 321 or consent of Course Coordinator

In this course students will learn advanced concepts for installing, configuring and securing various types of network servers including enterprise, web and mail servers. The course also covers the documentation of network systems infrastructure and the testing of hardware and software network components.

**CIT 420 Digital Forensics**
Prerequisite: CIT 415

An introduction to the fundamentals of computer forensics and cyber-crime scene analysis. The various laws and regulations dealing with computer forensic analysis will be discussed. Students will be introduced to the emerging international standards for computer forensic analysis, as well as a formal methodology for conducting computer forensic investigations.

**CIT 431 Applied Secure Protocols**
Prerequisites: CIT 303, CIT 120 or a course in discrete math, and CIT 220 or a course in probability or statistics

This course will emphasize the applied facets of cryptography for the information assurance and security professional. By the end of the course students will be able to apply important cryptographic principles and tools to allow networks to communicate securely.

**Selective**

With this selective, students will have the opportunity to supplement their studies with a course that relates to their individual security interests, or expands their knowledge in security-related areas. The following selective list is not all-inclusive - students may propose other classes as substitutes but must be prepared to demonstrate why those particular courses are suitable. Students are responsible for determining and meeting any prerequisites for these classes and note that prerequisites do not count toward certificate requirements.

BUS L203 - Commercial Law I (3 cr.)
BUS S507 - Management of Information Technology (1.5 hrs)
CIT 352 Decision Support and Information Systems (3 cr.)
CIT 402 Design and Implementation of Local Area Networks (3 cr.)
CIT 440 Communication Network Design (3 cr.)
CIT 490 Senior Project (3 cr.)
POLS Y311 Democracy and National Security (3 cr.)
SPEA J101 The American Criminal Justice System (3 cr.)
SPEA V160 National and International Policy (3 cr.)
SPEA V376 Law and Public Policy (3 cr.)

**Course Mappings**

The NSTISSC has established a set of standards for Information Systems Security professionals. These provide the minimum training and education standards for properly executing the duties and responsibilities of:

- Information Systems Security (INFOSEC) Professionals
- Designated Approving Authority (DAA)
- System Administration (SA) in Information Systems Security
- Information Systems Security Officers (IAD).

The Information Assurance Courseware Evaluation (IACE) assesses the curriculum against the 4011 NSTISSI 4011 National Training Standard for Information Systems Security (INFOSEC) Professionals. Meeting these standards is one requirement for the program to receive certification under the IACE. Obtaining this certification is one of the goals of our department, so that we may offer NSA certificates to our students. Thus these standards were used to map IA and security content to courses in the certificate. The specific course mappings are shown in Table 1 in Appendix A.

The standards are written to provide two levels of knowledge (NSTISSI No. 4011, 1994):

a. Awareness level. Creates a sensitivity to the threats and vulnerabilities of national security information and a recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and practices INFOSEC.
b. Performance level. Provides the employee with the skill or ability to design, execute, or evaluate agency INFOSEC procedures and practices. This level of understanding will ensure employees are able to apply security concepts while performing their tasks.

While not required to receive NSTISSI certification under the IACE, the network administration courses in the certificate were mapped to the NSTISSI 4013 standards (1997). These mappings are shown in Table 2 in Appendix A.

**3. List the major student outcomes (or set of performance-based standards for the proposed certificate).**

The major goal of this program is to provide an efficient and effective method for transitioning students into the security profession. Participants completing this program will have a solid foundation in the techniques used for security. The NSTISSI standards provide a set of outcomes that will be followed in order for the student to gain all the necessary tools to supply security in the network and systems environment. The hands-on nature of this program will allow graduates to immediately apply the knowledge and skills learned as network security administrators.

A secondary goal of this program is to upgrade the skills of current network and system administrators in the area of information assurance and security. Security and security

techniques are changing on a regular basis and this program will provide a viable option for network and systems administrators to stay current.

**4. Explain how student outcomes will be assessed (course-embedded assessments, graduate follow-up, employer survey, standardized tests, etc.):**

The following means will used to evaluate the students' declarative and procedural knowledge gained as they advance through the certificate program:

- Lab projects. Students will be required to participate in security labs to re-enforce the techniques and approaches taught.
- Quizzes and examinations will be conducted that cover security technologies and techniques.
- The students will be required to maintain a network procedure and troubleshooting journal.

**5. Describe the student population to be served.**

This certificate is designed to meet the needs of three groups of students: CIT majors, non-majors and professional network and systems administrators.

CIT majors can use the certificate to develop a specialty in Information Assurance. Required courses for CIT majors will supply students with the necessary prerequisites for the certificate. All of the courses in the certificate will easily fit into the Networking and Standard tracks without adding any credit hours. Students in the Networking track have expressed interest in this area.

Non-majors with an interest in Information Assurance can pursue the certificate, with the completion of 6-9 hours of prerequisite coursework in Data Communications (CIT 307, CIT 336, and math knowledge).

The certificate is ideal mechanism for current systems and networking professionals to add or update their Information Assurance knowledge. Three or more years of relevant professional experience would meet the certificate prerequisites. The certificate is designed so that it can be completed within one calendar year. This allows professionals working in security to complete the certificate in a timely manner.

**6. How does this certificate complement the campus or departmental mission?**

The Network Security Certificate will complement the mission of the Department of Computer and Information Technology by providing quality education for a larger, more diverse student population from a variety of working areas and cultures. These courses will not only be elements of a stand-alone program, they will also be integrated into the CIT curriculum. CIT students as well as Certificate students can benefit from these courses.

The proposed certificate program will fulfill the campus mission in much the same way as it complements the goals of the CIT department. The certificate program will place IUPUI in a

position to respond to the fast-paced technological environment, the needs of the community and the alumni within the community.

This program will also complement the mission of IUPUI by, most specifically, contributing to university efforts to develop much needed security education. The department, campus, and university will benefit from the increased visibility and accessibility created by this certificate program.

**7. Describe any relationship to existing programs within Indiana University.**

As far as can be determined, no other certificate program exists within the Indiana University system that presents the same content or delivery method as this proposed CIT program. A search has uncovered the following individual courses in security offered at IUPUI:

- CSCI 590 Network Security (3 cr.)
- ECE 595 Computer Security (3 cr.)
- BUS A580 E-Commerce Security and Control (1.5 cr.)

The first two are graduate level courses focused particularly to their majors. The last is a survey course that is part of the Business Professional Accountancy program in the Kelly School of Business.

This certificate would be the first comprehensive program in network security for technology.

**8. List and indicate the resources required to implement the proposed program. Indicate sources, e.g., reallocations or any new resources such as personnel, library holdings, equipment, etc.).**

Connie Justice will be responsible for the leadership and management of this program. Ms. Justice did most of the development of the Networking track, developed all of the hands-on components for current networking courses, and has 16 years of professional networking experience. Dr. Eugenia Fernandez will provide the academic and curriculum development oversight for this certificate. Their capabilities have been proven through the successful development and implementation of the Networking track, a highly popular program.

For subject matter expertise, senior personnel will be deployed as follows:

| Faculty | Topics |
|---|---|
| Connie Justice | Security, Network and Systems Administration |
| Andrew Korty | Security |
| Christie Minns | Data Communications |
| Dave Dellacca | Data Communications, Networking |

Senior personnel (subject matter experts) will be responsible for instructional content creation, labs and assessment of student learning.

Connie Justice is currently working with Cisco Systems on a grant to acquire network security equipment.

**9. Describe any innovative features of the program (e.g., involvement with local or regional agencies, offices, etc., cooperative efforts with other institutions, etc.):**

A collaboration effort is currently underway with Texas A&M Commerce and Purdue University, West Lafayette in which the schools are developing course curriculum and security labs for CIT 406 Advanced Network Security and exchanging the content between the schools. The labs are being developed by CIT. Texas A&M is supplying lecture material developed by their graduate students.

CIT and CERIAS are collaborating on CIT 420 Digital Forensics where course content is exchanged and a faculty member from Purdue West Lafayette will be commuting to Indianapolis to teach the course for CIT next Spring.

**References**


Dark, M. (n.d.). Overview of the Purdue University project. Retrieved October 1, 2003 from Purdue University, Center for Education and Research in Information Assurance and Security: http://www.cerias.purdue.edu/education/post_secondary_education/undergrad_and_grad/faculty_development/info_assurance_education/overview_purdue.php

*Information Assurance Education Graduate Certificate Program* (n.d.) Retrieved October 2, 2003 from Purdue University, Center for Education and Research in Information Assurance and Security: http://www.cerias.purdue.edu/education/post_secondary_education/undergrad_and_grad/faculty_development/info_assurance_education/

*National INFOSEC Education & Training Program - Information Assurance Courseware Evaluation Process.* (n.d.). Retrieved October 2, 2003 from the National Security Agency, INFOSEC website: http://www.nsa.gov/isso/programs/nietp/corseval.htm

NSTISSI No. 4011. (20 June 1994). National Training Standard for Information Systems Security (INFOSEC) Professionals. Washington, DC: National Security Telecommunications and Information Systems Security Committee. Retrieved October 2, 2003 from http://www.nstissc.gov/Assets/pdf/4011.pdf

*Overview of the NSA IAATREP Program.*(n.d.). Retrieved October 1, 2003 from Purdue University, Center for Education and Research in Information Assurance and Security: http://www.cerias.purdue.edu/education/post_secondary_education/undergrad_and_grad/faculty_development/info_assurance_education/overview_nsa.php

Spanninger, M.K. (2001, May). Developing security competencies through information assurance undergraduate and graduate programs. Paper presented at the 5th National Colloquium for Information Systems Security Education, Fairfax, VA. Retrieved October 1, 2003 from. http://cisse.info/CISSE%20J/2001/Span.pdf

| Table 1 - NSTISSI 4011 Mappings for the Network Security Certificate | | | | |
|---|---|---|---|---|
| | **CIT 303 Comm. Security and Network Controls** | **CIT 406 Advanced Network Security** | **CIT 431 Applied Secure Protocols** | **CIT 420 Digital Forensics** |
| **a. COMMUNICATIONS BASICS (Awareness Level)** | | | | |
| (a) Historical vs Current Methodology | | | | |
| (b) Capabilities and limitations of various communications systems | | | | |
| **b. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS** | | | | |
| (a) Historical vs Current Technology | | | | |
| (b) Hardware | | | | |
| (c) Software | | | | |
| (d) Memory | | | | |
| (e) Media | | | | |
| (f) Networks | | | | |
| **c. SECURITY BASICS (Awareness Level)** | | | | |
| (a) INFOSEC Overview | | | | |
| (b) Operations Security (OPSEC) | | | | |
| (c) Information Security | | | | |
| (d) INFOSEC | | | | |
| **d. NSTISS BASICS (Awareness Level)** | | | | |
| (a) National Policy and Guidance | | | | |
| (b) Threats to and Vulnerabilities of Systems | | | | |
| (c) Legal Elements | | | | |
| (d) Countermeasures | | | | |
| (e) Concepts of Risk Management | | | | |
| (f) Concepts of System Life Cycle Management | | | | |
| (g) Concepts of Trust | | | | |
| (h) Modes of Operation | | | | |
| (i) Roles of Various Organizational Personnel | | | | |
| (j) Facets of NSTISS | | | | |
| **e. SYSTEM OPERATING ENVIRONMENT (Awareness Level)** | | | | |
| (a) AIS | | | | |
| (b) Telecommunications Systems | | | | |
| (c) Agency Specific Security Policies | | | | |
| (d) Agency Specific AIS and Telecommunications Policies | | | | |
| **f. NSTISS PLANNING AND MANAGEMENT (Performance Level)** | | | | |
| (a) Security Planning | | | | |
| (b) Risk Management | | | | |
| (c) Systems Life Cycle Management | | | | |
| (d) Contingency Planning/Disaster Recovery | | | | |
| **g. NSTISS POLICIES AND PROCEDURES (Performance Level)** | | | | |
| (a) Physical Security Measures | | | | |

| Table 1 - NSTISSI 4011 Mappings for the Network Security Certificate | | | | |
|---|---|---|---|---|
| | **CIT 303 Comm. Security and Network Controls** | **CIT 406 Advanced Network Security** | **CIT 431 Applied Secure Protocols** | **CIT 420 Digital Forensics** |
| (b) Personnel Security Practices and Procedures | | | | |
| (c) Software Security | | | | |
| (d) Network Security | | | | |
| (e) Administrative Security Procedural Controls | | | | |
| (f) Auditing and Monitoring | | | | |
| (g) Cryptosecurity | | | | |
| (h) Key Management | | | | |
| (i) Transmission Security | | | | |
| (j) TEMPEST Security | | | | |

| Table 2 - NSTISSI 4013 Mappings for the Network Security Certificate | | |
|---|---|---|
| | CIT 415 Advanced Network Administration | CIT 406 Advanced Network Security |
| **1. GENERAL** | | |
| **a. Security Policy** | | |
| (1) define local accountability policies; | | |
| (2) explain accreditation; | | |
| (3) discuss three agency specific security policies; | | |
| (4) define assurance; | | |
| (5) explain certification policies as related to local requirements; | | |
| (6) define local e-mail privacy policies; | | |
| (7) describe local security policies relative to electronic records management; | | |
| (8) explain security policies relating to ethics; | | |
| (9) describe relevant FAX security policies; | | |
| (10) discuss the concept of information confidentiality; | | |
| (11) identify information ownership of data held under his/her cognizance; | | |
| (12) identify information resource owner/custodian; | | |
| (13) define local information security policy; | | |
| (14) describe information sensitivity in relation to local policies; | | |
| (15) discuss integrity concepts; | | |
| (16) describe local policies relevant to Internet security; | | |
| (17) explain local area network (LAN) security as related to local policies; | | |
| (18) define policies relating to marking of sensitive information; | | |
| (19) understands fundamental concepts of multilevel security; | | |
| (20) describe policies relevant to network security; | | |
| (21) define the functional requirements for operating system integrity; | | |
| (22) perform operations security (OPSEC) in conformance with local policies; | | |
| (23) explain physical security policies; | | |
| (24) discuss local policies relating to secure systems operations; | | |
| (25) identify appropriate security architecture for use in assigned IS(s); | | |
| (26) describe security domains as applicable to local policies; | | |
| (27) define local policies relating to separation of duties; | | |
| (28) identify systems security standards policies; | | |
| (29) identify DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), or Orange Book policies; | | |
| (30) identify TEMPEST policies; | | |
| (31) define TEMPEST policies; | | |
| (32) define validation and testing policies; | | |
| (33) identify verification and validation process policies; | | |
| (34) define verification and validation process policies; | | |
| (35) describe wide area network (WAN) security policies; | | |
| (36) use/implement WAN security policies; | | |
| (37) describe workstation security policies; | | |
| (38) use/implement workstation security policies; and | | |
| **b. Procedures** | | |
| (1) practice/use facility management procedures; | | |
| (2) describe FAX security procedures; | | |
| (3) practice/use FAX security procedures; | | |
| (4) describe housekeeping procedures; | | |

| Table 2 - NSTISSI 4013 Mappings for the Network Security Certificate | | |
|---|---|---|
| | CIT 415 Advanced Network Administration | CIT 406 Advanced Network Security |
| (5) perform housekeeping procedures; | | |
| (6) describe information states procedures; | | |
| (7) distinguish among information states procedures; | | |
| (8) explain Internet security procedures; | | |
| (9) use Internet security procedures; | | |
| (10) explain marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms, March 30, 1987); | | |
| (11) perform marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms, March 30, 1987); | | |
| (12) apply multilevel security; | | |
| (13) explain the principles of network security procedures; | | |
| (14) use network security procedures; | | |
| (15) describe operating system integrity procedures; | | |
| (16) perform operating systems security procedures; | | |
| (17) assist in local security procedures; | | |
| (18) describe purpose and contents of National Computer Security Center TG-005, Trusted Network Interpretation (TNI), or Red Book; | | |
| (19) describes secure systems operations procedures; | | |
| (20) define TEMPEST procedures; | | |
| (21) identify TEMPEST procedures; | | |
| (22) identify certified TEMPEST technical authority (CTTA); | | |
| (23) describe WAN security procedures; | | |
| (24) practice WAN security procedures; and | | |
| (25) explain zoning and zone of control procedures. | | |
| **c. Education, Training, and Awareness** | | |
| (1) discuss the principle elements of security training; | | |
| (2) explain security training procedures; | | |
| (3) explain threat in its application to education, training, and awareness; | | |
| (4) use awareness materials as part of job; | | |
| (5) distinguish between education, training, and awareness; | | |
| (6) give examples of security awareness; | | |
| (7) give examples of security education; | | |
| (8) discuss the objectives of security inspections/reviews; and | | |
| (9) identify different types of vulnerabilities. | | |
| **d. Countermeasures/Safeguards** | | |
| (1) discuss the different levels of countermeasures/safeguards assurance; | | |
| (2) describe e-mail privacy countermeasures/safeguards; | | |
| (3) define Internet security; | | |
| (4) describe what is meant by countermeasures/safeguards; | | |
| (5) describe separation of duties; | | |
| (6) define countermeasures/safeguards used to prevent software piracy; | | |
| (7) define TEMPEST countermeasures/safeguards; and | | |
| (8) explain what is meant by zoning and zone of control. | | |
| **e. Risk Management** | | |
| (1) explain ways to provide protection for Internet connections; | | |

| Table 2 - NSTISSI 4013 Mappings for the Network Security Certificate | | |
|---|---|---|
| | CIT 415 Advanced Network Administration | CIT 406 Advanced Network Security |
| (2) describe operating system integrity; | | |
| (3) define TEMPEST as it relates to the risk management process; | | |
| (4) identify different types of threat; | | |
| (5) explain WAN security; and | | |
| (6) explain what zoning and zone of control ratings are based on. | | |
| **2. ACCESS CONTROL** | | |
| **a. Policies/Administration** | | |
| (1) use network access controls as designed; | | |
| (2) explain compartmented/partitioned mode; | | |
| (3) describe data access; | | |
| (4) identify the dedicated mode of operation; | | |
| (5) explain electronic records management; | | |
| (6) define information ownership; | | |
| (7) identify information resource owner/custodian; | | |
| (8) describe separation of duties; and | | |
| (9) define the system high mode. | | |
| **b. Countermeasures** | | |
| (1) describe use of caller ID; | | |
| (2) give five examples of countermeasures; | | |
| (3) define internal controls and security; | | |
| (4) identify methods of intrusion detection; | | |
| (5) define network firewalls; and | | |
| (6) describe network security software. | | |
| **c. Safeguards** | | |
| (1) demonstrate the ability to use alarms, signals, and reports; | | |
| (2) identify network security software; | | |
| (3) describe operating system security features; | | |
| (4) define protected distribution systems; and | | |
| (5) describe system security safeguards. | | |
| **d. Mechanisms** | | |
| (1) discuss authentication mechanisms; | | |
| (2) describe discretionary access controls; | | |
| (3) describe mandatory access controls; | | |
| (4) describe one-time passwords; | | |
| (5) discuss privileges; and | | |
| (6) define single sign-on. | | |
| **ADMINISTRATIVE** | | |
| **a. Policies/Procedures** | | |
| (1) identify basic/generic management issues; | | |
| (2) define change control policies; | | |
| (3) discuss documentation; | | |
| (4) explain electronic records management; | | |
| (5) describe object reuse; | | |
| (6) define operational procedure review; | | |
| (7) discuss policy enforcement; | | |
| (8) identify procedures; | | |
| (9) discuss security inspections; and | | |

| Table 2 - NSTISSI 4013 Mappings for the Network Security Certificate | | |
|---|---|---|
| | CIT 415 Advanced Network Administration | CIT 406 Advanced Network Security |
| (10) describe local password management policy. | | |
| **b. Countermeasures/Safeguards** | | |
| (1) give examples of alarms, signals and reports; | | |
| (2) define application development control; | | |
| (3) assist in preparing assessments; | | |
| (4) identify countermeasures; | | |
| (5) describe disaster recovery procedures; | | |
| (6) discuss disposition of classified information; | | |
| (7) practice disposition of media and data; | | |
| (8) practice document labeling; | | |
| (9) discuss proper use of security safeguards; | | |
| (10) define separation of duties; | | |
| (11) identify storage media protection and control; and | | |
| (12) define system software controls. | | |
| **4. AUDIT** | | |
| **a. Policies/Procedures** | | |
| (1) use alarms, signals and reports in accordance with existing policies and procedures; | | |
| (2) summarize audit-related documentation; | | |
| (3) discuss electronic records management relative to compliance with local policies and procedures; | | |
| (4) describe three policies and/or procedures in which separation of duties is appropriate or mandatory. | | |
| **b. Countermeasures/Safeguards** | | |
| (1) identify two countermeasures applicable to audit trail tampering; and | | |
| (2) describe three safeguards gained through use of audit trails. | | |
| **c. Tools** | | |
| (1) explain two major benefits of auditing; | | |
| (2) identify three audit tools; | | |
| (3) describe the major benefit gained through use of audit trails and logging policies; | | |
| (4) define an error log; | | |
| (5) explain two capabilities offered by expert security/audit tools; | | |
| (6) identify two intrusion detection systems; and | | |
| (7) describe the major operating system security features. | | |
| **5. OPERATIONS** | | |
| **a. Policies/Procedures** | | |
| (1) describe disaster recovery policies and procedures; | | |
| (2) use/implement disaster recovery policies and procedures; | | |
| (3) define disaster recovery policies and procedures; | | |
| (4) describe documentation policy and procedures; | | |
| (5) use/implement documentation policy and procedures; | | |
| (6) discuss object reuse policy and procedures; | | |
| (7) describe separation of duties policies and procedures; | | |
| (8) practice/implement separation of duties policies and procedures; | | |
| (9) identify disposition of media and data policies and procedures; | | |
| (10) perform disposition of media and data policies and procedures; | | |

| Table 2 - NSTISSI 4013 Mappings for the Network Security Certificate | | |
|---|---|---|
| | CIT 415 Advanced Network Administration | CIT 406 Advanced Network Security |
| (11) explain disposition of media and data policies and procedures; and | | |
| (12) identify storage media protection/control policies and procedures. | | |
| **b. Countermeasures/Safeguard** | | |
| (1) use countermeasure/safeguard alarms, signals and reports; | | |
| (2) describe countermeasures; | | |
| (3) use/implement countermeasures/safeguards; | | |
| (4) discuss countermeasure/safeguard corrective actions; | | |
| (5) assist in performing countermeasure/safeguard corrective actions; | | |
| (6) describe safeguards; and | | |
| (7) use/implement safeguards. | | |
| **c. Management/Oversight** | | |
| (1) use/implement management/oversight change controls; | | |
| (2) describe configuration management; | | |
| (3) discuss database integrity; | | |
| (4) describe disaster recovery management/oversight; | | |
| (5) use/implement disaster recovery management/oversight; | | |
| (6) discuss electronic records management/oversight; | | |
| (7) identify the key elements of information integrity; | | |
| (8) discuss information management; | | |
| (9) explain risk management; and | | |
| (10) practice risk management. | | |
| **6. CONTINGENCY** | | |
| **a. Continuity of Operations** | | |
| (1) practice backups; | | |
| (2) describe continuity planning; | | |
| (3) describe disaster recovery; | | |
| (4) describe disaster recovery plan testing; and | | |
| (5) discuss disaster recovery planning. | | |
| **b. Countermeasures/Safeguards** | | |
| (1) use alarms, signals and reports; | | |
| (2) define information availability; | | |
| (3) identify examples of corrective actions; | | |
| (4) select countermeasures; | | |
| (5) identify methods of intrusion detection; and | | |
| (6) select appropriate safeguards. | | |
| **c. Configuration Management** | | |
| (1) practice change controls; | | |
| (2) explain database integrity; | | |
| (3) practice disposition of classified info; | | |
| (4) perform disposition of media and data; | | |
| (5) perform electronic records management; | | |
| (6) practice emergency destruction; and | | |
| (7) identify storage media protection and control procedures. | | |

3/17/04 Review Committee appointed-- Walston, Stephen L; Mac Kinnon, Joyce L; Mccreary, W. M; Kuzcowski, Joseph
3/25/04 Science requested that the review be delayed. Trudy Banta will add it to her list of topics to deal with.
5/7/04 Review comments presented by J Kuzcowski and R Porter

Indiana University Purdue University Indianapolis
Academic Policies and Procedures Committee
Guidelines for Review of New Degree Proposals

When the chair of the APPC is informed that an academic unit is preparing a new degree proposal, this document will be sent to the Dean of the unit to inform the faculty of the areas that are reviewed by the APPC. Item 10 (program evaluation plan) may require the proposing unit to develop a brief addition to the information requested in the ICHE new degree proposal format.

APPC will not review a new degree proposal unless a representative of the proposing academic unit is present to answer questions during the APPC meeting.

A working group of APPC members will be assigned as 'primary reviewers' of the proposal and will prepare a summary report for distribution to the APPC prior to the scheduled discussion of the proposal. The summary will be distributed without attribution to those involved in preparing the report. All members of APPC are expected to review the proposal prior to the discussion.

In the review of the New Degree Proposal, the APPC will consider the following items.

1) **Does the Program Description clearly describe the new degree?**
   a) Purpose is 'to provide Information Assurance education and training to students and professionals'. (p 1)
   b) Curriculum was developed so that 'the program can receive formal certification from the National INFOSEC Education and Training Program segment of NSA [National Security Agency]' which will allow IUPUI to issue Information Systems Security certificates to individuals who complete the program.

2) **Does the statement of the program's goals and objectives clearly differentiate this degree from other degrees at IUPUI?**
   **a)** Potential overlaps with School of Science programs have been resolved.

3) **Are the admission requirements and enrollment restrictions consistent with other IUPUI programs? If not, is the rationale clearly presented?**
   a) Certificate can be completed within 1 year by individuals working in security
      i) Admissions criteria (p 2)
         (1) AS in technology area with knowledge of basic data communication concepts, discrete math, and probability or statistics
            (a) AS in CIT

(b) AS in other subject plus CIT 307, CIT 120 and 220, or equivalents

(2) Professional certification in network and system administration such as a Microsoft Certified System Engineer

(3) 3 or more years of experience in network and systems administration

That is, anyone meeting current UCOL admissions standards can be admitted and take the intro courses. To go beyond that they would have to go through the department (right now, Connie Justice) to be able take the advanced courses. The only exception would be that students with an A.S. or B.S. in CIT, ECET, or CSCI could be admitted directly into the certificate.

(4)

b) Courses in the certificate program can be applied to Bachelor's degree in Computer and Information Technology

**4) Are the degree requirements consistent with other IUPUI programs?**

a) Consists of six 3-credit hour courses
   i) Three are currently taught
   ii) Two are under development
   iii) One course from a selective list

**5) Is the sample curriculum consistent with similar IUPUI degree programs?**

**a)** Curriculum is consistent with other IUPUI certificate programs

**6) Does the curriculum have potential positive or negative impact on the enrollment in the courses or degrees in other academic units?**

a) Three courses were identified with related content. All are taught at the graduate level.

**7) Will the faculty resources dedicated to the program have positive or negative impact other academic units?**

a) The faculty resources deployed in the proposed courses are internal to the Department of Computer and Information Technology.

**8) Does the program rationale support the institutional need for the degree?**

a) The certificate responds the shortage of skilled information assurance professionals in the workforce by providing a mechanism for those in the workforce to complete the certificate as well as incorporating the content with the CIT course offerings.

**9) Is it likely that this degree will compete with existing degrees for students?**

a) The certificate will enroll CIT majors, non-majors with an interest in Information Assurance, and professional network and systems administrators.

**10) Is the program evaluation plan consistent with the learning outcome assessment strategies used by other IUPUI degree programs?**

a) 'The NSTISSI standards provide a set of outcomes that will be followed in order for the student to gain all the necessary tools to supply security in the network ans systems environment.' (p 4)

b) Mapping course content to the NSTISSI standards set by the NSTISSC permits the program to receive formal certification from the National INFOSEC Education and Training Program segment of the NSA so that INFOSEC certificates can be issues to students who complete the program. (p 1-2)
c) Description of assessment of student learning during program included.
d) No plans for graduate follow up or employer survey included
e) The evaluation plan should include strategies for program assessment in addition to student assessment