### INSTRUCTIONS:

Please check the items below which describe the purpose of this request.

- [ ] New course with supporting documents (complete proposal form)
- [X] Add existing course offered at another campus
- [ ] Expiration of a course
- [ ] Change in course number
- [ ] Change in course title
- [ ] Change in course credit/type
- [7] Change in course attributes
- [8] Change in instructional hours
- [9] Change in course description
- [10] Change in course requisites
- [11] Change in semesters offered
- [12] Transfer from one department to another

### PROPOSED:

- Subject Abbreviation: CIT
- Course Number: 528
- Long Title: Information Security Risk Assessment
- Short Title: Info Sec Risk Assess

### EXISTING:

- Subject Abbreviation: CIT
- Course Number: 528
- Long Title: Information Security Risk Assessment
- Short Title: Info Sec Risk Assess

### TERMS OFFERED:

- [X] Summer
- [X] Fall
- [X] Spring

### CAMPUS(ES) INVOLVED:

- Calumet
- Cont Ed
- Ft. Wayne
- [X] Indianapolis
- [X] N. Central
- [X] Tech Statewide
- [X] W. Lafayette

### CREDIT TYPE:

- 1. Fixed Credit: Cr. Hrs. 3
- 2. Variable Credit Range: Minimum Cr. Hrs. (Check One) To Or
- 3. Equivalent Credit: Yes
- 4. Thesis Credit: Yes

### COURSE ATTRIBUTES:

- 1. Pass/Not Pass Only
- 2. Satisfactory/Unsatisfactory Only
- 3. Repeatable
- 4. Credit by Examination
- 5. Designator Required
- 6. Special Fees

### INSTRUCTIONAL TYPE:

- Lecture
- Recitation
- Presentation
- Laboratory
- Lab Prep
- Studio
- Distance
- Clinic
- Experiential
- Research
- Ind. Study
- Pract/Observ

### COURSE DESCRIPTION (INCLUDES REQUISITES):

Covers information security risk assessment, including the following topics: steps in performing information security risk assessment, threats to information security, technical, managerial, and operational vulnerabilities, methods for analyzing controls, methods for determining likelihood of and impact from an information security breach, and methods for determining risk. Emphasizes the development and utilization of security metrics in the risk assessment process.

Prerequisites: Graduate standing
New Course Request

Check Appropriate Boxes: Undergraduate credit [ ] Graduate credit [X] Professional credit [ ]

1. School/Division: School of Engr and Tech

2. Academic Subject Code: CIT

3. Course Number: 528 (must be cleared with University Enrollment Services)

4. Instructor: Justice, C

5. Course Title: Information Security Risk Assessment

Recommended Abbreviation (Optional): Info Sec Risk Assess

6. First time this course is to be offered (Semester/Year): Fall 2008

7. Credit Hours: Fixed at 3 or Variable from ________ to ________

8. Is this course to be graded S-F (only)? Yes [X] No [ ]

9. Is variable title approval being requested? Yes [ ] No [X]

10. Course description (not to exceed 50 words) for Bulletin publication:

   Covers information security risk assessment, including the following topics:
   - steps in performing a risk assessment; threats to information security;
   - technical, managerial, and operational vulnerabilities; methods for analyzing
   controls and information security breaches; and methods for determining risk.
   - Emphasizes the development and utilization of security metrics.

11. Lecture Contact Hours: Fixed at 3 or Variable from ________ to ________

12. Non-Lecture Contact Hours: Fixed at 0 or Variable from ________ to ________

13. Expected enrollment: 15, of which 90% percent are expected to be graduate students.

14. Frequency of scheduling: every 3 semesters. Will this course be required for majors? No

15. Justification for new course: This course is an elective course for the new M.S. Technology program.

16. Are the necessary reading materials currently available in the appropriate library? Yes.

17. Please append a complete outline of the proposed course, and indicate instructor (if known), textbooks, and other materials.

18. If this course overlaps with existing courses, please explain with which courses it overlaps and whether this overlap is necessary, desirable, or unimportant.

19. A copy of every new course proposal must be submitted to departments, schools, or divisions in which there may be an overlap of the new course with existing courses or areas of strong concern, with instructions that they send comments directly to the originating Curriculum Committee. Please append a list of departments, schools, or divisions thus consulted.

Submitted by:

[Signature] Date 5-3-2007

Department Chairman/Division Director

[Signature] Date

Dean of Graduate School (when required)

Approved by:

[Signature] Date 5/9/07

Dean

[Signature] Date

Chancellor/Vice-President

[Signature] Date

University Enrollment Services

After School/Division approval, forward the last copy (without attachments) to University Enrollment Services for initial processing, and the remaining four copies and attachments to the Campus Chancellor or Vice-President.

UPS 724 University Enrollment Services Final—White; Chancellor/Vice-President—Blue; School/Division—Yellow; Department/Division—Pink; University Enrollment Services Advance—White
Course List >> West Lafayette >> Traditional Programs >> C&IT - Computer And Information Technology

Search Summary: 0 retired courses, 1 current course, and 0 courses to be activated in the future.

Effective dates of retired items appear in *italicized red*; effective dates of current items appear in black; effective dates of future items appear in *bolded green*.

Show Retired | Hide Current | Hide Future

C&IT 528 - Information Security Risk Assessment

**Information** 05/15/2006 - Forward

**Effective:**

**Credits:** 3.00

**Typical Instructional Format:** Lecture that meets once per week for 150 minutes per meeting for 16 weeks.

**Usually Offered:** Spring

**Short Title:** Info Sec Risk Assess

**Description:** Covers information security risk assessment, including the following topics: steps in performing information security risk assessment, threats to information security, technical, managerial, and operational vulnerabilities, methods for analyzing controls, methods for determining likelihood of and impact from an information security breach, and methods for determining risk. Emphasizes the development and utilization of security metrics in the risk assessment process.

**Registration Approval:** Instructor approval is required.

**School:** College Of Technology

**Department:** Computer And Information Technology

**Credit By Exam:** Credit by examination is not available for this course.

**Replaces** CPT 528

All contents Copyright 2007 Purdue University. All rights reserved. This is an Official World Wide Web page of Purdue University. Suggestions and comments about it may be directed to: registrar@purdue.edu.

I. HEADER:

Course Number: CIT 528
Title: Information Security Risk Assessment

Instructor: Connie Justice
Office: SL 220
Phone: 278.3830
Email: cjustice@iupui.edu

Prerequisites: Graduate status in the School of Technology

II. COURSE DESCRIPTION AND RATIONALE:

Description

Covers information security risk assessment, including the following topics: steps in performing information security risk assessment, threats to information security, technical, managerial, and operational vulnerabilities, methods for analyzing controls, methods for determining likelihood of and impact from an information security breach, and methods for determining risk. Emphasizes the development and utilization of security metrics in the risk assessment process.

III. EDUCATIONAL OBJECTIVES:

Upon successful completion of this course, students will be able to:

- Identify and prioritize information assets.
- Identify and prioritize threats to information assets.
- Define an information security strategy and architecture.
- Plan for and respond to intruders in an information system.
- Explain legal and public relations implications of security and privacy issues.
- Present a risk assessment plan using a published assessment standard.
- Prepare a risk assessment plan.
- Present a risk assessment plan.
- Explore IT’s impact on work, workers, and the workforce.

IV. COURSE CONTENT:

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic(s)</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction; Effective Risk</td>
<td></td>
</tr>
<tr>
<td>Analysis; Introduction to Security Management</td>
<td>In Class Assignment 1</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td>Effective Risk Analysis; Introduction to Security Management</td>
<td>In Class Assignment 2</td>
<td></td>
</tr>
<tr>
<td>Systems/Security Life Cycle; Planning</td>
<td>Homework 1</td>
<td></td>
</tr>
<tr>
<td>Planning for Contingencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Policies</td>
<td>In Class Assignment 2</td>
<td></td>
</tr>
<tr>
<td>Security Policy Writing</td>
<td>In Class Assignment 3</td>
<td></td>
</tr>
<tr>
<td>Compliance Presentation</td>
<td>Seminar Topic Presentation</td>
<td></td>
</tr>
<tr>
<td>Security Programs</td>
<td>Homework 2</td>
<td></td>
</tr>
<tr>
<td>Security Management Models and Practices</td>
<td>Client Risk Assessment Assignment</td>
<td></td>
</tr>
<tr>
<td>Risk Management: Identifying and Assessing Risk and demo</td>
<td>Client Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>Threat and Vulnerability Identification Lecture and demo</td>
<td>Client Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>Control Analysis and Likelihood determination and demo</td>
<td>Client Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>Impact Analysis and Risk Determination</td>
<td>Client Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>Control Recommendations Assessment Results</td>
<td>Client Risk Assessment</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment Presentation</td>
<td>Final Binders Due</td>
<td></td>
</tr>
</tbody>
</table>

V. **REQUIRED AND RECOMMENDED TEXTS:**

Management of Information Security  
Herbert Mattord, Michael Whitman  
Publish date: January 27, 2004  
Course Technology

Information Security Risk Analysis (BOOKS 24x7)  
Thomas R. Peltier  
Auerbach Publications © 2001 (281 pages)  
ISBN:0849308801

Managing a Network Vulnerability Assessment (Books 24x7)  
by Thomas R. Peltier, Justin Peltier and John A. Blackley  
Auerbach Publications © 2003  
ISBN:0849312701
VI. EVALUATION AND GRADING:

<table>
<thead>
<tr>
<th>Component</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midterm</td>
<td>200</td>
</tr>
<tr>
<td>In Class Assignment</td>
<td>40-50</td>
</tr>
<tr>
<td>Homework</td>
<td>50-100</td>
</tr>
<tr>
<td>Final Presentation</td>
<td>125</td>
</tr>
<tr>
<td>Final Poster</td>
<td>50</td>
</tr>
</tbody>
</table>

Grading Scale

A Represents the highest grade possible and indicates outstanding achievement. This grade is not automatically given to the top student performance but instead indicates student work which demonstrates complete mastery of course learning objectives or evinces a level of creativity or originality which far exceeds course expectations. The grade indicates the student works independently and with strong initiative, seeking knowledge outside the normal framework of the course.

B Represents achievement considerably above expectations. Student performance demonstrates thorough understanding of course learning objectives and a high level of creativity or originality.

C Student performance meets designated course requirements and demonstrates understanding of the course material and attainment of the course learning objectives. This is the grade that may be expected of a student who puts forth a reasonable amount of time and effort and completes all requirements.

D This grade denotes substandard work and indicates incomplete and inadequate understanding of the course learning objectives. It indicates work which may not satisfy all requirements.

F This grade indicates serious deficiency in understanding course learning objectives and failure to complete requirements of the course.
VIII. CHEATING AND PLAGIARISM:

Indiana University has adopted a code that applies, with only minor differences, to students on all Indiana University campuses. The code, which is available in the Office of the Dean of Students and in all school office, spells out what constitutes unacceptable behavior and the procedures to be followed when there are alleged cases of misconduct. The dean of students also has some very brief pamphlets on key areas of the code. What follows is not the code but rather abbreviated and paraphrased statements on key elements of the code: academic and personal misconduct as well as a section on what students should do if they believe that other students, faculty, or staff have violated their rights. The code also explains the procedures employed and how students may appeal decisions. For more information, consult the Code of Student Rights, Responsibilities, and Conduct as well as brochures located in the Office of the Dean of Students.

Indiana University Purdue University Indianapolis Code of Conduct

Cheating of any kind will be grounds for failure. You are allowed to discuss your assignments with others. However, you are expected to submit your own work for grading. You are expected to create your own assignments independent of others except when directed to work in teams. Do not cheat. The submission of false computer output is also considered to be cheating.

Cheating will not be tolerated. Cheating and/or plagiarism will be immediately punished with a grade of zero for the assignment in question, reported to the Chairman of the Department of Computer and Information Technology and a letter describing the infraction will be placed in your student file. Further disciplinary action will be pursued according to university policy as described in Part III of the Code of Student Rights, Responsibilities, and Conduct (Issued August 15, 1997).

Instructors using software to detect plagiarism are encouraged to investigate whether or not the student’s permission is needed.

VIII. AMERICANS WITH DISABILITIES ACT:

If you need any special accommodations due to a disability, please contact Adaptive Educational Services at (317)-274-3241. The office is located in CA 001E.
Dear Eugenia,

The School of Informatics had the opportunity to review CIT 528 Information Security Risk Assessment and CIT 550 Organizational Impact of Information Technology courses that CIT is planning to offer.

We fully support the development and offering of these courses and we hope that Informatics students may in fact benefit from these two new course offerings.

Sincerely,

Mathew Palakal
Associate Dean, Research & Graduate Programs
Director, Informatics Research Institute
School of Informatics

From: Fernandez, Eugenia
Sent: Tuesday, July 03, 2007 12:18 PM
To: Palakal, Mathew J.
Cc: Lim, Wai-Sei Valerie
Subject: Request for Support of New Courses

Dean Palakal,

We have submitted several new course requests in support of our new M.S. in Technology program. The Graduate Curriculum Sub-Committee has requested a letter of support from your school with respect to the following courses:

- CIT 528 Information Security Risk Assessment
- CIT 550 Organizational Impact of Information Technology

I have attached the submitted course materials for your review. A letter of support can be as informal as a return email or a formal memo addressed to the Graduate Curriculum Sub-Committee – either way is acceptable.

If I have reached the wrong person with this request, please let me know who I should contact.

Thank you.

Eugenia Fernandez, Ph. D.
Director, M.S. in Technology Program

Computer & Information Technology
Purdue School of Engineering and Technology, IUPUI
799 W. Michigan St., ET 301
Indianapolis, IN 46202-5160

317.274.6794 Voice