PURDUE UNIVERSITY
REQUEST FOR ADDITION, EXPIRATION,
OR REVISION OF AN UNDERGRADUATE COURSE
(100-400 LEVEL)

DEPARTMENT: Computer and Electrical Engineering Technology &
Information Systems and Technology
EFFECTIVE SESSION: Fall / 2010

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

☐ 1. New course with supporting documents
☐ 2. Add existing course offered at another campus
☐ 3. Expiration of a course
☐ 4. Change in course number
☐ 5. Change in course title
☐ 6. Change in course credit/type
☐ 7. Change in course attributes (department head signature only)
☐ 8. Change in instructional hours
☐ 9. Change in course description
☐ 10. Change in course requisites
☐ 11. Change in semesters offered (department head signature only)
☐ 12. Transfer from one department to another

PROPOSED:
Subject Abbreviation: IST
Course Number: 430
Long Title: IT Security and Risk Management
Short Title: IT Security and Risk Management

EXISTING:
Subject Abbreviation:  
Course Number:  

TERMS OFFERED:
Check All That Apply:
☒ Summer ☐ Fall ☑ Spring

CAMPUS(ES) INVOLVED:
☒ Calumet ☐ Cont Ed ☐ Tech Statewide
☒ Ft. Wayne ☐ Ind. Indianapolis

CREDIT TYPE
1. Fixed Credit Cr. Hrs.: 3.0
2. Variable Credit Range: Minimum Cr. Hrs. (Check One) To ☐ Or ☑ Maximum Cr. Hrs.
3. Equivalent Credit: Yes ☑ No ☐
4. Thesis Credit: Yes ☑ No ☐

COURSE ATTRIBUTES: Check All That Apply
1. Pass/Not Pass Only 7. Registration Approval Type
2. Satisfactory/Unsatisfactory Only 8. Department
3. Repeatable 9. Instructor
5. Designator Required 10. Honors
6. Credit by Examination 11. Full Time Privilege
8. Variable Title 12. Off Campus Experience
5. Special Fees

Instructional Type
Lecture: Min. Meetings Per Week: 75 16
Recitation: 2
Presentation:  
Laboratory:  
Lab Prep:  
Studio:  
Distance:  
Clinic:  
Experiential:  
Research:  
Ind. Study:  
Pract/Observe:  

% of Credit Offered: 100
% of Credit Allocated:  
Delivery Method: (Asyn. Or Syn.)  
Delivery Medium: (Audio, Internet, Live, Text-Based, Video)  
Cross-Listed Courses:  

COURSE DESCRIPTION (INCLUDE REQUIREMENTS):
P: IST 350. This course provides an introduction to the fundamental principles and topics of Information Technology Security and Risk management at the organizational level. Students will learn critical security principles that enable them to plan, develop, and perform security tasks. The course will address hardware, software, processes, communications, applications, and policies and procedures with respect to organizational IT Security and Risk Management.

Calumet Department Head  
Date: 10/24/09
Calumet School Dean  
Date:  

Ft. Wayne Department Head  
Date:  
Ft. Wayne School Dean  
Date:  

Indianapolis Department Head  
Date:  
Indianapolis School Dean  
Date:  

North Central Department Head  
Date:  
North Central Chancellor  
Date:  

West Lafayette Department Head  
Date:  
West Lafayette College/School Dean  
Date:  
West Lafayette Registrar  
Date:  

OFFICE OF THE REGISTRAR
Learning objectives

Students will:

1. Understand the fundamental principles of Information Technology security.
2. Understand the concepts of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.
3. Understand the need for the careful design of a secure organizational information infrastructure.
4. Understand risk analysis and risk management.
5. Understand both technical and administrative mitigation approaches.
6. Understand the need for a comprehensive security model and its implications for the security manager.
7. Understand both technical and administrative mitigation approaches.
8. Gain an understanding of security technologies.
9. Gain an introductory understanding of basic cryptography, its implementation considerations, and key management.
10. Learn to design and guide the development of an organization’s security policy.
11. Learn to determine appropriate strategies to assure confidentiality, integrity, and availability of information.
12. Learn to apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.

Topics

- Introduction to Information Security
  - Inspection
    - Resource Inventory
    - Threat Assessment
    - Identifying Vulnerabilities
    - Assigning Safeguards
  - Protection
    - Awareness
    - Access
    - Identification
    - Authentication
    - Authorization
    - Availability
    - Accuracy
    - Confidentiality
    - Accountability
    - Administration
  - Detection
    - Intruder Types
    - Intrusion Methods
    - Intrusion Process
    - Detection Methods
    - Monitoring Systems
- Reaction
o Incident Determination
o Incident Notification
o Incident Containment
o Assessing Damage
o Incident Recovery
o Automated Response

• Reflection
  o Incident Documentation
  o Incident Evaluation
  o Legal Prosecution

• Risk Assessment Frameworks
  o COSO Integrated Control Framework
  o CoBiT – ISACA
  o Australia/New Zealand Standard – Risk Management
  o ISO Risk Management – Draft Standard

• Security Engineering
  o Protocols
  o Passwords
  o Access Controls
  o Cryptography

• Physical Aspects
  o Biometrics
  o Physical Tamper Resistance
  o Security Printing and Seals

• Security in Connected Systems and Networks
  o Distributed Systems
  o Telecom System Security
  o Network Attack and Defense
  o Protecting E-Commerce Systems

• Policy and Management Issues
  o Copyright and Privacy Protection
  o E-Policy

Discussion

• The use of case examples for discussion and reflection in this course is highly recommended.

• It is recommended to include an applied project for a potential client in which students conduct a risk assessment of a part of the client’s IT infrastructure.