Professor: Ray Trygstad
Address: IIT Daniel F. and Ada L. Rice Campus, 201 E Loop Rd., Wheaton, IL 60187
Telephone: 630.447.9009
Fax: 630.682.6010
Email: trygstad@iit.edu
Offices: Rice Campus - Rice Room 227
Main Campus - Perlstein Hall 10 W 33rd St, Room 233D
Office Hours: Rice Campus: Thursday 3:00-5:00pm
Main Campus: Tuesday 2:00-4:00pm
Online: Via GoogleTalk (username trygstad) or by telephone to 630.447.9009
or by text message to 630.666.7348

Course Catalog Description: In-depth examination of topics in the management of information technology security including access control systems & methodology, business continuity & disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models. Graduate students will be required to complete a research paper.

Prerequisites: None
Credit: 3-0-3 Semester Hours

Lecture Day, Time & Place: Thursday 6:25pm to 9:05pm at IIT's Rice Campus Room 163, or online via IIT Online.

Course Objectives: Each successful student will demonstrate foundation knowledge and application of information system (IS) security concepts as they to apply the management of IS security in a large organizational environment. Students will describe and identify policy frameworks, legal and moral implications, and best practices in information security management. Students will be able to conduct a security audit of an organization and report on the results with appropriate suggestions for amelioration of problem areas identified.

Schedule of Topics/Readings: You should do all readings prior to class.

<table>
<thead>
<tr>
<th>Session</th>
<th>Date</th>
<th>General Topic</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>August 28</td>
<td>Introduction to Information Security</td>
<td>Chapter 1</td>
</tr>
<tr>
<td>2</td>
<td>September 4</td>
<td>Planning for Security</td>
<td>Chapter 2</td>
</tr>
<tr>
<td>3</td>
<td>September 11</td>
<td>Security Policy</td>
<td>Chapter 4</td>
</tr>
<tr>
<td>4</td>
<td>September 18</td>
<td>Risk Management I</td>
<td>Chapter 8</td>
</tr>
<tr>
<td>5</td>
<td>September 25</td>
<td>Risk Management II</td>
<td>Chapter 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Graduate research paper outline due</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>October 2</td>
<td>The Information Security Audit</td>
<td>Online</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Undergraduate paper 1 due</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>October 9</td>
<td>Disaster Recovery &amp; Business Continuity</td>
<td>Chapter 3</td>
</tr>
<tr>
<td>8</td>
<td>October 16</td>
<td>Developing Security Programs</td>
<td>Chapter 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(SIGITE: Lecture will be online only and class will not meet)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Graduate research paper bibliography due</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>October 23</td>
<td>Security Management Models</td>
<td>Chapter 6</td>
</tr>
<tr>
<td>10</td>
<td>October 30</td>
<td>Security Management Practices</td>
<td>Chapter 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Undergraduate paper 2 due</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>November 6</td>
<td>Protection Mechanisms</td>
<td>Chapter 10</td>
</tr>
<tr>
<td>12</td>
<td>November 13</td>
<td>Personnel and Security</td>
<td>Chapter 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Graduate research papers due</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>November 20</td>
<td>Legal, Ethical &amp; Professional Issues</td>
<td>Chapter 12</td>
</tr>
<tr>
<td>14</td>
<td>November 27</td>
<td>Thanksgiving Holiday</td>
<td>No Class</td>
</tr>
<tr>
<td>15</td>
<td>December 4</td>
<td>IS Audit Class Presentations</td>
<td></td>
</tr>
<tr>
<td>Exam</td>
<td>December 11</td>
<td>Final Examination 7:30-9:30pm</td>
<td></td>
</tr>
</tbody>
</table>

Textbook: The textbook for this course is mandatory.
Readings: Readings for the class will be assigned from the textbook as well as in the form of handouts or online reading. It is essential that you do all readings before coming to class on the assigned date. Readings are a necessary and integral part of the class and will form the basis for any class discussions on the topic. Specific readings are assigned by topic above. Online resources will be linked from Blackboard or will be posted on Blackboard.

Course Notes: Copies of the course lecture notes in the form of a PDF of the PowerPoint presentation accompanying each lecture will be provided for each student on Blackboard. This should be useful if you must miss a class. You should be aware that note taking is encouraged and should help your understanding of the material.

Course Web Site: http://blackboard.iit.edu/

Blackboard: The course will make intensive use of Blackboard (http://blackboard.iit.edu/) for communications, assignment submissions, group project coordination, providing online resources and administering examinations. All remote students will view the course lectures online via Blackboard, and online readings will be found on Blackboard.

Guest Speakers: Guest speakers may be featured as part of course topics. When a guest speaker is expected you should make an extra effort to be seated and ready prior to class time. A question & answer/discussion period will be held at the end of each speaker’s presentation.

Attendance: If you are in a live section of the class (-01, -0FR or -0FV) and will not be able to attend class, please notify me via email or by text message to 630.447.9009 prior to class time. Live section students who miss a class should always watch the lecture online. One lecture, on October 16, will only be online due to the professor’s attendance at the ACM SIGITE conference.

Assignments: There will be two assignments for this class.

Assignment 1 - Graduate Students: A research paper addressing a topic in the management of information security. The paper can be a solution to a problem in cyber security, a discussion of a cyber security management strategy or a case study. The paper will be fifteen to twenty pages long and will meet standards expected of a paper submitted for journal publication. Instructions for submission of the paper will be included with the assignment on Blackboard. You must fully attribute all material directly quoted and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. Failure to format your bibliography entries in APA style will result in an automatic reduction of one letter grade for this assignment. No more than thirty-three percent of material included in any paper may be direct quotes. No more than sixty percent of the resources cited may be from online. Wikipedia may not be cited. Submission of the paper for actual publication is highly encouraged. A basic outline for your paper—which should be at least three pages in length—will be due September 25; a preliminary bibliography will be due October 16. The paper will be due November 13.

Assignment 1 - Undergraduate Students: Two three-page research papers each addressing a topic in information security in more depth than it may covered in the course. The three pages should be content and do not include cover page, bibliography, charts, diagrams, figures, appendices or other included materials. Topics should be of particular interest to you and may be more technical in nature than the course. Papers must have a complete bibliography citing a minimum of five sources other than the textbook or class notes. You must fully attribute all material directly quoted and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. Failure to format your bibliography entries in APA style will result in an automatic reduction of one letter grade for this assignment. No more than thirty-three percent of material included in any paper may be direct quotes. No more than sixty percent of the resources cited may be from online. Wikipedia may not be cited. These papers will be due October 2 and October 30.

Note: I will not provide topics for research papers. Topic selection is an important part of the research process. There is an enormous and expansive variety of topics in this field and with a little work on your part arriving at a topic should not be difficult at all. Topics should be very specific as you will be covering it in a relatively short amount of writing and you want to reflect an in-depth coverage of your topic which you can not do with a very broad topic.

TL;DR: Pick your own research paper topic. Broad topic = bad; specific, narrow topic = good.
ITMS/IT-S 478/578 Cyber Security Management
Fall 2012

Assignment 2: A Information Security Audit in which students in groups will conduct an Information Security Audit of an existing business, government agency or organization. Audits of businesses will not reveal the name of the business and students auditing a business must sign nondisclosure agreements prior to conducting the audit. The Audit Report will be in narrative form with appropriate suggestions for amelioration of problem areas identified, about ten pages long. and will be accompanied by a computer-based slide show when presented to the class. Internet students residing on Main Campus or in the Chicago area should make arrangements to attend class at Rice Campus in Wheaton on the due date to present their project. The IS Audit will be due December 4.

Quizzes: I may give quizzes at my discretion and may use them for verification that you have completed assigned reading. As they are discretionary, the weight of quizzes in grading is also left to my discretion and will be included in your class participation grade. Quizzes may be online via Blackboard.

Examinations: The final examination will consist of a take-home essay section and an in-class multiple choice examination measuring course outcomes as discussed above. Internet students residing in the Chicago area should make arrangements to attend the final examination at the Main Campus in Chicago or at the Rice Campus in Wheaton. Online students in the Chicago area who cannot attend the final exam during the scheduled final exam period due to a conflicting exam must make alternate testing arrangements with me. Internet students in remote locations will arrange for examination proctoring through IIT Online.

Plagiarism: All work you submit in this course must be your own. You must fully attribute all material directly quoted in papers and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. Including directly quoted material in an assignment without attribution is always plagiarism and will always be treated as such by me. No more than thirty-three percent of material included in any paper may be direct quotes. Students have submitted plagiarized material the last six times I have taught this course and I will not tolerate it. If you submit plagiarized material you WILL receive a grade of ZERO for the assignment, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies. There is no excuse for not understanding this policy and if you do not understand it please let me know and I will be happy to discuss it with you until you do.

Grading: Grading criteria for ITMS 478/IT-S 478 students will be as follows:

- **A**: Outstanding work reflecting substantial effort.................................................................90-100%
- **B**: Excellent work reflecting good effort..................................................................................80-89.99%
- **C**: Satisfactory work meeting minimum expectations...............................................................70-79.99%
- **D**: Substandard work not meeting expectations.........................................................................60-69.99%
- **E**: Unsatisfactory work...............................................................................................................0-59.99%

Grading criteria for ITMS 578 students will be as follows:

- **A**: Outstanding work reflecting substantial effort.................................................................90-100%
- **B**: Adequate work fully meeting that expected of a graduate student........................................80-89.99%
- **C**: Weak but marginally satisfactory work not fully meeting expectations...............................65-79.99%
- **E**: Unsatisfactory work...............................................................................................................0-64.99%

The final grade for the class will be calculated as follows:

- Assignment 1.............................................................................................................................30%
- Assignment 2.............................................................................................................................30%
- Final Exam.................................................................................................................................30%
- Quizzes/Class Participation.........................................................................................................10%

Other Class Resources: Online readings and other class resources may be found at on Blackboard.

Our Contract: This syllabus is my contract with you as to what I will deliver and what I expect from you. If I change the syllabus, I will issue a revised version of the syllabus; the latest version will always be available on Blackboard. Revisions to readings and assignments will be communicated via Blackboard.

Disabilities: Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. My office hours are listed on the first page of the syllabus. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312 567.5744 or disabilities@iit.edu.
Course Outcomes: These are lecture-by-lecture learning outcomes. When you complete this course, you should be able to:

**Lesson 01**
- Recall policies and requirements for his course
- Describe what information security is and how it came to mean what it does today
- Discuss the history of computer security and how it evolved into information security
- Identify and define key terms and critical concepts of information security
  - List the fundamental concepts of the Information Assurance/Cyber Defense discipline
  - List the first principles of security
  - Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies
- List and describe the phases of the system life-cycle.
- Outline the phases of the security systems development life cycle
- Describe who is involved in information security in an organizational structure
- Recall key elements of project management as they apply to security
- List and describe the elements of a maturity model
- Discuss the following topics:
  - The Building Security In Maturity Model; the Software Assurance Maturity Model; change control; terms including Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repubidiation, and Privacy; project management; the Security Life-Cycle; and System Life-Cycle Phases and Issues

**Lesson 02**
- Discuss the importance of planning
- Describe the principal components of organizational planning
- Know and understand the principal components of information security system implementation planning as it functions within the organizational planning scheme
- Describe the threats posed to information security and discuss the more common attacks associated with those threats
  - Describe characteristics of malware
  - Describe different types of attacks and their characteristics
  - Describe potential system attacks and the actors that might perform them
  - Describe why good human machine interfaces are important to system use
- Describe cyber defense tools, methods and components
- Differentiate threats to information systems from attacks against systems
- Examine the placement of security functions in a system and describe the strengths and weaknesses
- Understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms
- Discuss the following topics:
  - The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access); adversaries and targets; attacker motivations and techniques; CBK; C-Level Functions; data Security (in transmission, at rest, in processing); the definition of “vulnerability”; failures of procedures; making Cybersecurity part of the core organizational strategy; operational, tactical, and strategic planning and management; root causes of vulnerabilities; social engineering and social engineering vulnerabilities; threat information sources (e.g., CERT); threats and adversaries and their methods including password guessing & cracking, sniffing, spoofing, and session hijacking; vulnerabilities and risks including backdoors, trojans, viruses, wireless attacks, denial of service (DOS) attacks, distributed DOS, BOTs, MAC spoofing, web app attacks, 0-day exploits, buffer overflows, privilege escalation, and rootkits

**Lesson 03**
- Define information security policy and understand its central role in a successful information security program
- Know the three major types of information security policy often used and what goes into each type
- Develop, implement, and maintain various types of information security policies
  - Develop system specific plans for the protection of intellectual property

**Lesson 04**
- Define risk management and its role in the organization
- Use risk management techniques to identify and prioritize risk factors for information assets
- Assess risk based on the likelihood of occurrence and impact on an organization
- Document the results of risk identification
- Describe how risk relates to a system security policy
Describe various risk analysis methodologies
Discuss the following topics:
- Basic Risk Assessment;
- Risk Assessment/Analysis Methodologies;
- Risk management and Analysis;
- Risk Management Processes;
- Risk Measurement and Evaluation Methodologies

Lesson 05
- Compare the advantages and disadvantages of various risk assessment methodologies
- Select the optimal methodology based on needs, advantages and disadvantage
- Describe and select from risk mitigation strategy options to control risk
- Identify risk control classification categories
- Use existing conceptual frameworks to evaluate risk controls
- Evaluate and categorize risk
  - With respect to technology
  - With respect to individuals
  - In the enterprise
  - And recommend appropriate responses
- Formulate a cost benefit analysis as required
- Maintain and perpetuate risk controls
- Discuss specific approaches to managing risk, and locate more detailed information about them if and when necessary
  - OCTAVE
  - Microsoft
  - FAIR
  - ISO 27005
- Discuss the following topics:
  - Communication of Risk;
  - Risk Management Models;
  - Risk Mitigation Economics;
  - Risk Transference/Acceptance/Mitigation

Lesson 06
- Explain what an information security audit is
- Explain the relationship of information security policies to the audit process
- Describe how an information security audit is conducted
- Discuss knowledge required for members of an information security audit team
- Assess the effectiveness of a security program
- Conduct audits to determine compliance with laws
- Discuss the following topics:
  - Security mechanisms such as Identification/Authentication and Audit

Lesson 07
- Discuss the need for contingency planning
  - Describe appropriate measures to be taken should a system compromise occur
  - Describe major components of contingency planning
  - Create a simple set of contingency plans using Business Impact Analysis
    - Develop contingency plans for various size organizations to include: business continuity, disaster recovery and incident response
- Prepare and execute a test of contingency plans
- Describe the combined contingency plan approach
- Discuss the following topics:
  - Business Continuity; Disaster Recovery; events that indicate an attack is or has happened

Lesson 08
- Recognize and discuss organizational approaches to information security
- List and describe functional components of the information security program
- Determine how to plan and staff an organization’s information security program based on organization size
  - Develop a security program, identifying goals, objectives and metrics
  - Effectively manage a security program
  - Assess the effectiveness of a security program
- Evaluate internal and external factors that influence activities and organization of an information security program
- List and describe typical job titles and functions performed in the information security program
- Describe components of a security education, training, and awareness program and understand how organizations create and manage these programs
- Discuss the following topics:
  - Security Awareness, Training and Education; Security Baselines
Lesson 09
- Select from dominant information security blueprints, frameworks and information security management models, including U.S. government-sanctioned models
  - Describe how standards, such as the Orange Book, may be applied to the requirements for a sub-contractor or customer
- Explain why access control is an essential element of information security management
  - Develop system specific plans for the implementation of access controls
- Select an information security management model, and customize it to meet the needs of a particular organization
- Implement the fundamental elements of key information security management practices

Lesson 10
- List the elements of key information security management practices
- Describe the key components of a security metrics program
- Identify suitable strategies for the implementation of a security metric program
- Discuss emerging trends in the certification and accreditation of U.S. federal IT systems
  - Define certification and accreditation
  - Describe the DoD system certification and accreditation processes
- Discuss the following topics:
  - Certification Boards and Panels, components of the C&A process, DoD Policies and Directives, the NIST Risk Management Framework (SP800-37)

Lesson 11
- Describe cyber defense tools, methods and components
  - Describe how the fundamental concepts of cyber defense can be used to provide system security
  - Examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed
- Recall and describe access control approaches, including authentication, authorization, and biometric access controls
  - Develop system specific plans for patch and change management
  - Develop system specific plans for the implementation of access controls
- Define and identify the various types of firewalls and the common approaches to firewall implementation
- Discuss current issues in dial-up access and protection
- Identify and describe the types of intrusion detection systems and the two strategies on which they are based
- Describe the various concepts in network defense
- Implement network defense measures
- Discuss cryptography and encryption
  - Identify elements of a cryptographic system
  - Describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc
  - Describe differences between symmetric and asymmetric algorithms
  - Describe the application of cryptography in SSL, virtual private networks, secure storage, and other security applications
- Discuss the following topics:
  - Defense in Depth; layering of security mechanisms to achieve desired security; malicious activity detection; & forms of attack; “Appropriate Countermeasures”; security mechanisms (e.g., Identification/Authentication, Audit); implementing firewalls and VPNs; DMZs, Proxy Servers; Intrusion Detection and Prevention Systems; implementing IDS/IPS; Honeypots and Honeynets; minimizing exposure (Attack Surface and Vectors); Network Access Control (internal and external); network attacks (e.g., session hijacking, Man-in-the-Middle); network monitoring; Network Traffic Analysis; network security techniques and components: access controls, flow control, cryptography, firewalls, intrusion detection systems, etc.; OS and Application Updates; patching; Cryptography; Public Key Cryptography; Public Key Infrastructure; Key Management (creation, exchange/distribution); common Cryptographic Protocols; Symmetric Cryptography (DES, Twofish); applications of Cryptography; Certificates; Digital Signatures (Authentication); Virtual Private Networks

Lesson 12
- Identify skills and requirements for information security positions
- Recognize various information security professional certifications, and identify which skills are encompassed by each
- Describe and implement information security constraints on the general hiring processes
Explain the role of information security in employee terminations
Describe security practices used to control employee behavior and prevent misuse of information
Discuss the following topics:
Roles and Responsibilities of the Security Organization, InfoSec roles and players

Lesson 13
Differentiate between law and ethics
Describe the ethical foundations and approaches that underlie modern codes of ethics
Identify major national and international laws that relate to the practice of information security
List applicable laws and policies related to cyber defense
Describe major components of each pertaining to storage and transmission of data
Describe what the laws mandate and where they apply
List the applicable laws for compliance in a given situation
Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it
Describe the impact of legal/regulatory standards on a given system
Conduct audits to determine compliance with laws
Discuss the role of culture as it applies to ethics in information security
Access current information on laws, regulations, and relevant professional organizations
Discuss the following topics:
Laws and Authorities; State, US and international standards / jurisdictions; compliance with applicable laws and regulations; Computer Security Act; US Patriot Act; FERPA; FISMA; Gramm Leach Bliley; Sarbanes-Oxley; HIPAA; Americans with Disabilities Act, Section 508; Payment Card Industry Data Security Standard (PCI DSS); privacy (COPPA); data breach disclosure laws; Bring Your Own Device (BYOD) issues