ITMS 484/584 Governance, Risk and Compliance
Spring 2015

Instructor: Bonnie A. Goins
Address: IIT Rice Campus, Wheaton, IL
Home Phone: 630-387-9496
Fax: 630.682.6010
Email: bgoins@iit.edu, secureit2003@yahoo.com
Office Hours: By appointment

Course Catalog Description: This course is an in-depth examination of topics in information technology/information security governance, risk and compliance, including Information Assurance policies, standards and compliance, as well as the examination of security risk analysis and the performance of systems certification and accreditation. Regular homework assignments and completion of a research paper are required for this course.

Prerequisites: ITMS 478 or ITMS 578 Credit: 3-0-3 Semester Hours

Lecture Day, Time & Place: Main Campus, Room TBD, Monday 6:25-9:05 pm.

Schedule of Topics/Readings: All readings should be done prior to class.

<table>
<thead>
<tr>
<th>Class Session</th>
<th>Date</th>
<th>Topic</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>January 12</td>
<td>Introduction to Risk Analysis</td>
<td>TBD</td>
</tr>
<tr>
<td>2</td>
<td>January 19</td>
<td>No class: Martin Luther King Day</td>
<td>TBD</td>
</tr>
<tr>
<td>3</td>
<td>January 26</td>
<td>Risk Assessment/Analysis Methods</td>
<td>TBD</td>
</tr>
<tr>
<td>4</td>
<td>February 2</td>
<td>Risk Treatment Methods &amp; Economics</td>
<td>TBD</td>
</tr>
<tr>
<td>5</td>
<td>February 9</td>
<td>Risk Management Models and Processes</td>
<td>TBD</td>
</tr>
<tr>
<td>6</td>
<td>February 16</td>
<td>Risk Measurement, Evaluation and Communication</td>
<td>TBD</td>
</tr>
<tr>
<td>7</td>
<td>February 23</td>
<td>Information Assurance: Standards, Laws and Regulation</td>
<td>TBD</td>
</tr>
<tr>
<td>8</td>
<td>March 2</td>
<td>Information Assurance: Standards, Laws and Regulation</td>
<td>TBD</td>
</tr>
<tr>
<td>9</td>
<td>March 9</td>
<td>Legal, Regulatory and Standards Compliance</td>
<td>TBD</td>
</tr>
<tr>
<td>10</td>
<td>March 16</td>
<td>No class: Spring Break</td>
<td>TBD</td>
</tr>
<tr>
<td>11</td>
<td>March 23</td>
<td>Legal, Regulatory and Standards Compliance</td>
<td>TBD</td>
</tr>
<tr>
<td>12</td>
<td>March 30</td>
<td>Legal, Regulatory and Standards Compliance</td>
<td>TBD</td>
</tr>
<tr>
<td>13</td>
<td>April 6</td>
<td>Policies, Laws, Regulations and Ethics</td>
<td>TBD</td>
</tr>
<tr>
<td>14</td>
<td>April 13</td>
<td>Policies, Laws, Regulations and Ethics</td>
<td>TBD</td>
</tr>
<tr>
<td>15</td>
<td>April 20</td>
<td>Conducting Audits, Assessments and Certification/Accred.</td>
<td>TBD</td>
</tr>
<tr>
<td>16</td>
<td>April 27</td>
<td>Conducting Audits, Assessments and Certification/Accred.</td>
<td>TBD</td>
</tr>
</tbody>
</table>

Exam   April 27-May 8: Take home final and homeworks are due at 9:05 p.m. May 8.

Course Materials: Slide decks will be assigned by the instructor and posted to Blackboard for students to download.

Course Objectives: Each successful student will demonstrate foundation knowledge of governance, risk and compliance (GRC) concepts as they apply to legal, regulatory and standards-based environments, such as HIPAA, FISMA, NERC, PCI DSS, GLBA, SOX, FERPA, COPPA and others. Students will describe and identify policy frameworks, legal and compliance implications, and best practices as follows:

- Students will be able to describe how risk relates to a system security policy.
- Students will be able to describe various risk analysis methodologies.
- Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
• Students will be able to compare the advantages and disadvantages of various risk assessment methodologies.
• Students will be able to select the optimal methodology based on needs, advantages and disadvantages.
• Students will be able to describe the impact of legal/regulatory standards on a given system.
• Students will be able to describe how standards, such as the Orange Book, may be applied to the requirements for a sub-contractor or customer.
• Students shall be able to describe what the laws mandate and where they apply.
• Students will be able to conduct audits to determine compliance with laws.
• Students will be able to list the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data.
• Students will be able to describe their responsibilities related to the handling of information about vulnerabilities.
• Students will be able to describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.
• Students will be able to describe the DoD system certification and accreditation processes.
• Students will be able to define certification and accreditation.

Course Notes: Copies of the course lecture slides decks will be available on Blackboard. Additionally, they will be available online for use by remote students or if you have missed a class session. You should be aware that note taking is encouraged and should help your understanding of the material.

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

Blackboard: The course will make intensive use of Blackboard (http://blackboard.iit.edu/).

Readings: 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. Any online resources will be uploaded to Blackboard.

Homework: There will be homework assignments for this class. These assignments must be satisfactorily completed in order to pass this course and count for 30% of your grade. Suggested deadlines are given for completion of the homework, but no additional points will be deducted from the homework if it is turned in by the end of the class.

Paper or Project: There will be a paper or project required for this class. This paper must be satisfactorily completed in order to pass this course and counts for 30% of your grade. The paper or project is to be turned in by the end of the class.

Examinations: The final examination will consist of a take-home exam. The exam will be posted on Blackboard for you to download; students will have at least one week to complete the exam and may use any reference materials to complete the exams. Because the exam is administered as an open book exam, grading will be more rigorous for this final. This exam will count for 40% of your grade. The final exam must be satisfactorily completed in order for students to pass this course.

Extensions: Extensions will be granted for students not turning in all of the required work by the end of the term with a sufficient reason, such as illness or extreme job workload.

Plagiarism: All work submitted by students must be your own. Plagiarism may result in an automatic grade of “E”. All material directly quoted in papers must be fully attributed and all sources used in the preparation of the paper must be documented using APA-style bibliographic entries. No more than thirty-three percent of material included in any paper may be direct quotes.
Grading:

Grading criteria for 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:

- Homework ......................................................................................................................... 30%
- Paper ................................................................................................................................. 30%
- Final Exam ....................................................................................................................... 40%