

**UNIVERSITY OF NOTRE DAME**  
**Department of Management**  
**MGT 60730 – Technology Risk Management**  
**Fall 2007, Module 2**

---

|                      |                                     |                |                |
|----------------------|-------------------------------------|----------------|----------------|
| <b>Instructor:</b>   | Dr. John D’Arcy                     | <b>Office:</b> | 351 MCOB       |
| <b>E-mail:</b>       | jdarcy1@nd.edu                      | <b>Phone:</b>  | (574) 631-1735 |
| <b>Office Hours:</b> | T/TH 2:00 to 3:00 or by appointment |                |                |

**Description:** This course provides the foundation for understanding the key issues associated with protecting information assets, determining levels of protection and response to security incidents, and designing a consistent, reasonable technology risk management program. Topics include information security policy formulation and implementation; ethical, legal, and privacy issues; network security architecture and technologies; business continuity and disaster recovery; and information security staffing and personnel. The course emphasizes managerial decision making through analyzing information security problems and understanding effective solutions.

**Course Objectives:** Upon completion of this course, students should be able to:

- Recognize key information security issues that require management attention and effort in a modern business enterprise.
- Explain the current information security threat posture, and demonstrate an awareness of the likely evolution of security threats, regulations, and countermeasures.
- Understand the basic concepts of technology risk management, including the tools and techniques involved in risk analysis.
- Discuss the technical and human aspects of technology risk management.
- Know how ethical, legal, and privacy issues define the environment in which information technology is viewed.
- Evaluate the effectiveness of various technology risk control strategies from a cost-benefit perspective.
- Understand information security policy formulation and implementation.

**Required Textbook:** Michael W. Whitman and Herbert J. Mattord. Principles of Information Security, Second Edition. Thomson Course Technology, 2005. ISBN: 0-619-21625-5

A number of additional readings and materials will be distributed by the instructor or made available for download or photocopy.

**References:**

Andy Jones and Debi Ashenden. Risk Management for Computer Security – Protecting Your Network and Information Assets. Elsevier, 2005. ISBN: 0-7506-7795-3.

Marie Wright and John Kakalik. Information Security Contemporary Cases. Jones and Bartlett Publishers, 2007. ISBN: 0-7637-3819-0.

NIST Computer Security Special Publications: <http://csrc.nist.gov/publications/nistpubs/>

**Class Format:** Class time will be devoted to lecture and discussion. Attendance and participation in class discussions is an important part of the learning process in this class. Students are expected to acquire, read, and comprehend the assigned readings before class and come prepared to participate in meaningful discussion. Students are also expected to behave in a professional manner (e.g., come to class on time, turn off your cell phones, don't do homework for other classes, etc.). Participation/professionalism is worth 15% of the final course grade.

**Assignments:** In addition to course readings, there will be regular homework assignments, as well as two additional assignments described below. Several homework assignments will consist of case study analyses in which students are required to read a particular case and respond to a series of questions provided by the instructor. All homework assignments must be typed and handed in to the instructor as a hard copy at the beginning of class on the due date.

**Current Event Review Assignment:** Each student will prepare a short, 2-3 page, double-spaced 12 point font, summary of a current event article on a technology risk management topic. The topic can consist of any current technology, process, policy, or business issue, as long as it relates to the objectives of the course. The assignment is to read the article, digest and ensure proper understanding of the subject matter, prepare a summary paper about the article, and present it in class. Both the paper and presentation should deliver:

- A detailed description of what the event is;
- The source of the article(s);
- Your statement of relevance to course objectives;
- What you think the event means to the practice of technology risk management;

**Risk Assessment Group Project:** Working in small groups, students will perform a risk assessment using an organization of their choice. Use the NIST Special Publications 800-26 and 800-30 as a guide to prepare a report for management indicating the risks and vulnerabilities specific to their organization. The report should include diagrams and a risk matrix chart to help explain your findings. The assignment will consist of a formal report, 8-10 pages, double spaced, in 12 point font, delivered to the instructor and a PowerPoint presentation to the class.

**Final Exam:** There will be one exam given during this course. This exam will be given on *Tuesday, December 18<sup>th</sup>*.

**Grading:** Course grades will be assessed on the following basis:

|                               |     |
|-------------------------------|-----|
| Participation/Professionalism | 15% |
| Current Event Assignment      | 10% |
| Homework/Case Assignments     | 25% |
| Risk Assessment Project       | 25% |
| Final Exam                    | 25% |

**Philosophy on Honesty and Professional Behavior:** All class members are expected to abide by the *MBA Academic Honor Code* and the *MBA Code of Conduct*. Departures from the codes will result in significant grade reductions. Students are expected to work on homework assignments individually, unless otherwise specified by the instructor. Group projects will be

completed by assigned team members. Teams may not consult with other MBA students who are not part of the team about any facet of the project. No student should copy another student's work or represent work done by someone else as if it were his or her own.

**Late Assignment Policy:** Acceptance of any late assignments is at the discretion of the instructor and, at a minimum, will result in a letter grade reduction for the particular assignment.

**If you have a learning disability or need accommodations for any reason, please advise the instructor within the first week of class. Confidentiality will be maintained.**

### TENTATIVE COURSE SCHEDULE

| Date           | Textbook Readings  | Topics  |
|----------------|--|---|
| <b>Oct. 30</b> |  | - Course Overview and Expectations<br>- Risk Management Terminology   |
| <b>Nov. 1</b>  | Ch. 4 (109-125)<br>Ch. 1 (1-18, 30-31)<br>Ch. 2 (35-60); Ch. 4 (126-130) | - Asset Identification and Valuation<br>- Information Security History<br>- Categories of Threats               |
| <b>Nov. 6</b>  | Ch. 2 (60-68)  | - Attack Types<br>- <b>Case 1:</b> ChoicePoint  |
| <b>Nov. 8</b>  |  | - Attack Types (cont'd)<br>- Social Engineering   |
| <b>Nov. 13</b> | Ch. 3  | - Legal and Ethical Issues<br>- <b>Case 2:</b> Advo, Inc.   |
| <b>Nov. 15</b> | Ch. 4 (130-138)<br>Ch. 7 (317-331)                                       | - Legal and Ethical Issue (cont'd)<br>- Vulnerability Analysis<br>- Risk Calculation                            |
| <b>Nov. 20</b> | Ch. 4 (138-165)  | - Risk Control Strategies<br>- Cost-Benefit Analysis<br>- <b>Case 3:</b> Aetna                                  |
| <b>Nov. 27</b> | Ch. 5 (171-234)  | - Security Policy Formulation and Implementation<br>- Business Continuity Planning<br>- <b>Case 4:</b> iPremier |
| <b>Nov. 29</b> | Ch. 6 (239-268, 274-277)<br>Ch. 7 (281-317)                              | - Network Security Architecture<br>- Firewalls and Intrusion Detection Systems                                  |
| <b>Dec. 4</b>  | Ch. 8  | - Basics of Cryptography<br>- <b>Case 5:</b> Secom  |
| <b>Dec. 6</b>  | Ch. 11 (451-471)<br>Ch. 12 (500-511; 517-527)                            | - Security and Personnel<br>- Information Security Maintenance  |
| <b>Dec. 11</b> |  | - Penetration Testing<br>- Emerging Issues  |
| <b>Dec. 12</b> |  | - Risk Assessment Presentations<br>- Review for Final Exam  |
| <b>Dec. 18</b> | <b>Final Exam</b>  |   |