



## RIST403 – IT Disaster Planning and Recovery

### Master Course Syllabus

#### **Course Overview (QM Standards 1.2)**

**Course description:** This course provides the skills necessary to manage IT disaster recovery planning. The course focuses on the protection of information. Students will analyze risk, design a plan, and explore available technologies.

#### **Course Goals:**

- The student will be able to initiate steps for development of a Contingency Plan
- The student will be able to develop an Incidence Response Plan in writing
- The student will be able to develop a Disaster Recovery Plan in writing
- The student will be able to develop a Business Continuity Plan in writing

#### **Pre-Requisites (QM Standard 1.6)**

There are no course prerequisites for this course other than being an RBA (Regents Bachelor of Arts) student.

#### **Minimum Technical Requirements and Online Resources (QM Standards 1.5 & 1.7)**

In addition to a web browser (preferable Firefox) that is Blackboard compatible, you will need the other WVROCKS supported technologies outlined in the student policies section. You should know how to access and use Internet, WVROCKS, and Microsoft Office programs, and you will need to have consistent access to these technologies. You should know how to use email with attachments. You will also need a flash drive.

**Online Resources:** This course makes use of many online resources. I have made every effort to make sure the links I have are up-to-date. However, due to the changing nature of the web, you may find that a resource is temporarily unavailable or has been removed. If this should happen, please send me an email and I will find an alternative resource or modify the assignment accordingly.

#### **Instructor Information (QM Standards 1.8 & 5.3)**

Individual instructors complete this information.

#### **Virtual Office Hours**

I am available in my virtual office by appointment only. Send me an email to set up an appointment.

#### **Personal Commitment**

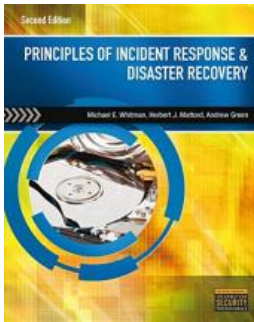
My personal commitments to you as a participant include:

- I will reply to course mail messages within 24 hours;
- I will read all discussion postings and will reply where appropriate within 3 days

- I will acknowledge my receipt of every course mail message immediately upon reading it. If I am unable to respond to the request or concern at the time of initial reply, I will give you an estimated time for my next reply.
- If I am going to be away from the course space for more than a day or two, I will send a message to you indicating the length of my absence.
- I will regularly update information regarding due dates in the course announcements.

## Optional/Required Course Materials (QM Standard 4.6)

Whitman, M.E., Mattord, H.J., and Green, A. (2013). *Principles of Incident Response and Disaster Recovery* (2nd ed.). Cengage Learning: Boston, MA.



This book provides an overview of contingency operations and its components as well as a through treatment of the administration of the planning process for incident response, disaster recover, and business continuity. It can be used to support course delivery for information-security-driven programs targeted at information technology students, as well as IT management and technology management curricula aimed at business or technical management students (Whitman, Mattord & Green, 2013). It is available at Marshall bookstores and online booksellers, and is available to rent.

Supplemental Required Readings in each unit provide additional information about course topics.

## Grading Policy (QM Standard 3.2)

The following types of assessments are included in the course:

**Assignments:** One assignment is required for each unit, with Assignment 4 being a group assignment. Assignments involve the practical application of the topics covered in each unit and will take some time. Each assignment is worth 50 points.

**Discussions:** Each unit contains two Discussion topics. Discussion Board postings provide the opportunity to share what you learned, or experienced if you are a working professional. Questions or scenarios will be posed to get the discussions started. I will monitor board activity to assure everyone is actively participating and contributing. The content of the online discussion may be used for quizzes. Please do not copy entire sections of an article as your contribution. It is better to provide a link to the article and discuss how the article relates to the course and discussion topic.

To participate in a discussion, you are required to post a response to each discussion topic at least twice per week. You have the opportunity to earn up to 25 points for each discussion topic. Your posted contribution will be graded for quality and relevance according to the rubric in the Grading section.

**Quizzes:** The course includes one quiz per unit. All quizzes are open book and timed. Quiz questions are based on assigned readings and may include discussion topics. You may use these sources while taking your quiz. However, keep an eye on the clock, as quizzes must be completed once started and have time restrictions. Each quiz is worth 25 points.

Discussion Board Participation	200 points (8 @ 25 points each)
Assignments	200 points (4 @ 50 points each)
Quizzes	100 points (4 @ 25 points each)
	500 total points

To calculate your grade, divide your points by 5 and compare to this scale for the letter-grade equivalent:

A = 90 –100;

B = 80 – 89;

C = 70 – 79;

F = < 70

## **Course Schedule and Weekly Outline**

### Unit 1:

- Chapters 1-3. This unit provides an introduction to computer security and risk management; contingency planning; and Business Impact Analysis.
- Unit 1 discussions, assignment and quiz are due during this time.
- Read Chapters 1-3 and Supplemental Reading
- Participate in 2 Discussions
- Complete Assignment 1
- Take Quiz 1

### Unit 2:

- Chapters 4-6. This unit focuses on incident response planning and detection; decision-making; and organizing the Computer Security Incident Response Team (CSIRT).
- Unit 2 discussions, assignment and quiz are due during this time.
- Read Chapters 4-6 and Supplemental Reading
- Participate in 2 Discussions
- Complete Assignment 2
- Take Quiz 2

### Unit 3:

- Chapters 7-9. This unit covers response planning, recovery and maintenance; and preparing for a disaster.
- Unit 3 discussions, assignment and quiz are due during this time.
- Read Chapters 7-9 and Supplemental Reading
- Participate in 2 Discussions
- Complete Assignment 3
- Take Quiz 3

### Unit 4:

- Chapters 10-12. This unit discusses disaster recovery challenges; crisis management; and continuity planning.

- Unit 4 discussions, assignment and quiz are due during this time.
- Read Chapters 10-12 and Supplemental Reading
- Participate in 2 Discussions
- Complete Assignment 4
- Take Quiz 4