UNIVERSITY OF PHOENIX
(UTAH)

UNIVERSITY OF PHOENIX COURSE SYLLABUS
CMGT 579 RISK MANAGEMENT, MODULE VERSION E-RK

This syllabus accompanies the above U of P Course module but supersedes it as a contract between students and the instructor where differences occur. The changes reflect concepts of increased need for business continuity rather than after the fact computer system recovery. The assignments have changed to emphasize the post Y2K e-commerce environment. These changes will provide a detailed base of information on technologies, issues and processes that can be the base line data for the CMGT 579 Strategic Planning course.

REQUIRED TEXTS

Bruce, G. and Demsey, R. **Security in Distributed Computing**.
Wold, J. and Shriver R. **Disaster-Proof Your Business**.

INSTRUCTOR Michael C. Helmantoler, B.A., BYU, M.A., BYU. Doctoral Candidate W.V.U. Michael Helmantoler is Certified Business Continuity Planner. He has 6 years experience in the field of disaster planning, emergency operations and contingency planning. He is a Senior Consultant with Strohl Systems Group the premier Business Impact Assessment and Disaster Planning software provider. Mr. Helmantoler is a crisis manager and an information technology systems integrator. He has experience with a wide range of hardware and software technologies in complex mainframe and distributed systems based solutions. He has successfully managed complex enterprise-wide software development, and is expert in identifying the operational impacts of the loss of communications, power and transportation systems. He served on three national disasters and five local disaster operations. He has developed continuity plans in finance, insurance, health care industry sectors. He is a member of the program committee of the Utah Association of Contingency Planners. He is a member of the Utah Seismic Safety Commission and the multi-hazard planning committee of the Safe Schools Leadership Consortium. He has taught undergraduate and graduate courses at Brigham Young University; Southern Illinois University; West Virginia University. His masters and doctoral research focused on at-a-distance-learning. He teaches graduate courses in information technology risk assessment and strategic planning for the University of Phoenix.

CONTACTING THE INSTRUCTOR

Telephone 801-785-7692 (home/office) Email Address <helmantole@aol.com>
Availability To ensure understanding of course requirements, to offer assistance and suggestions meet with me after class or by email at <helmantole@aol.com>

Session 1

10 min.	Quiz on reading assignment using notes only.
1 hr.	Explanation how each course assignment integrates into the final business continuity plan.
½hr.	Team formation and assignments of individuals to functional areas for detailed analysis.
½hr.	Roles of security and business resumption planning in the organizational environment.

¼hr. Individual oral reports on interesting internet addresses, (URLs), dealing with security topics.
¼hr. Management objectives of a security program.
¼hr. Management objectives for business continuity plans.
¼hr. Security exposures present to critical business processes.
¼hr. Individual oral report on effects of five common computer viruses.

Session 2

¼hr Quiz on reading assignment using notes only.

Turn in assignment: The Risk Assessment Paper/Table consists of 3 to 4 pages in table format rather than narrative text. This is an individual assignment with each person on the team taking a different business unit i.e.: accounting operations, distribution, customer care, market research, etc. Each business unit will be described in a paragraph addressing the potential threat that would cause an interruption (Loss of telecom due to cut cable, 48 hour power outage, fire on the floor housing the business unit, breach of computer security). Table 1 Business Impact Analysis Of Time Critical Processes. Row for each process. Columns recovery priority, recovery time objective, critical employees, equipment, telecom, vital records, vendors, software.

Process	Priority	Recover	Employees	Equipment	Telecom	Vital records	Vendor	Software	etc
Payroll	2	8 hrs	Time Clerk	ADP terminal	875-5678	W4	ADP	Timecr	
			Acct Pay Mgr	Modem	225-7854	Allotments	Zion’s	Banco	
Receivables	3	72 hrs	Acct. Rec. Clerk	Telephone	875-6665	Invoices	Bond	Collect	
			Collector	Telephone	875-9934	CB Report	TRW	Xtalk	

Tables 2-7 for each column in Table 1 (employees, equipment, telecom vital records, vendors, software, supplies.) Create a table for (critical employees, equipment, telecom, vital records, vendors, software, supplies, locations).

Each table will have different columns to describe the recovery asset i.e.:
Critical employees: Position, address, home phone, work phone, cell phone, pager, shift called by, calls who
Equipment (Fax machine, copiers, telephone sets): Description, manufacturer, supplier, model, sub model
Telecom: Description, type of line, speed, protocol closest location, label
Vital records: Description, Location, Media, Type (permanent, 7 yr, 3 yr) Confidentiality,
Vendors: Corp Name, Address, Phone 1, Phone 2, Service, Product, Account #, Sales Rep, Alternative Vendor
Software: Vendor, description, release, version number, supplier. Supplies: description, quantity on hand, vendor
Locations: Alternative suitable for business unit critical personnel, Type(storage, command post) services, functions located there,
1 hr Discuss findings identified in individual Risk Assessment paper.
1 hr Determining levels of critically in systems, Developing a recovery strategy.
1 hr Costs and benefits of risk assessment. Techniques of Business Impact Analysis
¼hr Types of security breaches that must be addressed and overcome in distributed computing environments.

Session 3

10 min. Quiz on reading assignment using notes only.

1 hr. Individual report on effects that the introduction of the Internet has on target organization’s security. Select a topic from each column and prepare several feature or benefits tables. Vulnerabilities: Denial of service; Cyber vandalism; Password cracking; Rogue ActiveX applets; Rogue Java applets; Exploiting NT and UNIX holes; Network denial of service; Password guessing Countermeasures: Vulnerability analysis and assessment; Firewalls; Encryption; Authentication; Intrusion detection.

1 hr. Managing, administering and controlling the security program in distributed processing.

1 hr. How to effectively report results of business impact analyses to C level management.

½hr. Individual research and writing assignments for Group comprehensive security plan development.

½hr.

Session 4

10 min. Quiz on reading assignment using notes only.

1 hr. Group 15 min. Security Plan Presentations.

1 hr. Peer EDP audit of other Group’s security plans for control requirements computer networks.

½hr. Successful staffing, strategy & requirements for business impact analysis. IPP

½hr. Tools, methods, and procedures for business interruption mitigation planning. IPP

½hr. How to organize and manage planning, crisis mgt, response and recovery teams. IPP

½hr. Individual research and writing assignment for Fault tolerant computing and design alternatives. Select one of the following: Clustering (parallel processing); Hot site backups; SANs; RAID (Redundant Array of Inexpensive Disks); Mirroring used in conjunction with other FT systems; Transaction logging and prepare several feature or benefits tables.

Session 5

10 min. Quiz on reading assignment using notes only.

1 hr. Individual Fault tolerant 5 minute presentations.

½hr. Lessons learned from mitigating risks related to the Y2K in information systems.

½hr. Managing a security violation incident with business continuity plans.

½hr. Group 1 peer evaluation of draft Disaster Recovery Paper.

½hr. Group 2 peer evaluation of draft Disaster Recovery Paper.

½hr. Group 3 peer evaluation of draft Disaster Recovery Paper.

½hr. Common benefits of integrating the security and disaster recovery functions.

Session 6

10 min. Quiz on reading assignment using notes only.

½hr. Group 1 Disaster Recovery Presentation.

½hr. Group 2 Disaster Recovery Presentation.

½hr. Group 3 Disaster Recovery Presentation.

1 hr. Budget justification for a business continuity planning effort.

½hr. Maintenance issues and assignments for business continuity plans.

½hr. Course Evaluation.

Assignments The assignments reflect continuity rather than recovery and the post Y2K e-commerce environment.

Grading

	Point Value for Assignments	
Assignment	**Workshop Submitted**	**Points Possible**
Weekly Reading Quizzes	All	30
Individual report on Security URLs, Viruses	1	3
Individual Business Unit Risk Assessment Paper	2	10
Individual Internet Security Paper	3	10
Group Security Paper and Presentation	4	10
Individual. Fault Tolerance technology Paper	5	10
Leveraging Y2K contingency planning into continuity plans	5	10
Business Continuity Plan Presentation	6	10
Participation	All	12
Total Possible		115

Overall Point Value for Course Grade 95-100 = A, 94 -91 = A-, 90-87 = B+, 86-83 = B, 82-79 = B-, 78-75 = C+, 74-71 = C, 70-67 = C- 66-63 = D+, 62-59 = D, 58 -55 = D-, 54 and lower = F.

Course Standards

- At least one assignment must be sent to the instructor each week to be considered in attendance for that week.
- All assignments will be prepared in Microsoft software and submitted as attachments to email. Assignments will be returned in the same manner.
- To substitute for the weekly discussion of the reading assignment, the student will prepare a 10 question multiple choice quiz that covers each of the topics listed in the session description. The student will prepare the quiz in MS Word and * the correct answers and indicate the book and page reference for each correct answer.
- Study Group project leadership experience will be gained by actual contact with a convenient security and disaster recovery/ business continuity professional in preparation and presentation of the project.
- The Security project will be carried out by interviewing an actual security officer.
- The Disaster Recovery Plan will be prepared in conjunction with an actual Disaster Recovery Manager.
- All assignments except those designed as “group” are meant to be individual efforts.
- Group efforts are meant to be equal efforts of all group members.
- All papers must be submitted on their due date.
- All documents are to be typed, spell-checked and grammar-checked, submitted double-spaced, and prepared in the proper format required for the program.
- Papers and project materials should avoid the revelation of company private, competition sensitive and confidential subjects of the companies in which the students are employed.
- Student will have received the necessary corporate approval if the papers and projects require the inclusion of any information about the company, its employees, business processes, and issues facing it.

- Particularly avoid the following violations of academic honesty.
  - Having a tutor or friend complete a portion of your assignments.
  - Having a reviewer make extensive revisions to an assignment.
  - Copying work submitted by another to a class as an assignment.
  - Using information from any data base service or internet source without proper citation or credit.

Attendance/Participation

- Attendance at class meetings is required. Any absence will affect student's course grades.
- A grade of "W" or "WF" to students with more than one absence in a course.
- Each group member must participate in a substantive role during each group presentation.

Written Assignments

All written assignments are due for the workshop for which they are assigned. Full letter grade reductions may result if papers are late. Graded elements of written assignments.

1. Titles, headings and subheadings to organize the papers per the UOP assignment module.
2. Typed double-spaced and in the format recommended in this module or discussed by the instructor.
3. Proof read for writing errors, spell checked and grammar checked.
4. Do not use report covers.