CIS 523/423
Disaster Recovery – Business Continuity

Course Description A study of disaster recovery and business continuity as related to the information technology function in organizations. Topics will include (but not limited to) security risk evaluation and management, creation of threat profiles, continuity of operations planning, contingency planning, and incident reporting.

Text Guide to Disaster Recovery, Michael Erbschloe, Thomson Course Technology. ISBN 0-619-13122-5

Course Objectives To provide theoretical knowledge and background about the key issues relating to disaster recovery and business continuity as related to information systems. This will be done through case analyses, research and the study of current and emerging techniques and technologies.

Course Learning Objective:

Create a notification directory.
Understand what is involved in getting management support.
Describe and understand the process involved in securing resources.
Explain how to prepare your resources.
Define the risks that may impact your organization.
Investigate different risk assessments and business impact assessments.
Set priorities for preventive measures and the recovery from any disaster situation.
Choose a risk assessment method to be used to identify and quantify risk in an organization.
Perform risk assessments as they might pertain to an organization.
Use tools such as OCTAVE to assist in risk assessment.
Identify all assets and functions in the organization.
Prioritize disaster recovery efforts based on assets and functions.
Differentiate between tier 1, tier 2, and tier 3 recovery targets to prioritize systems that must be recovered in the event of a disaster.
Determine dependencies between different data, functions, and assets.
Distinguish between an inconvenient situation and a true disaster using disaster declaration threshold criteria.
Determine the best way or ways to back up your data so that it can be recovered later.
Evaluate your off-site storage options.
Acknowledge information as well as hardware and software as an asset.
Determine recovery site options.
Examine recovery site types.
Develop recovery site selection criteria.
Outline a recovery solution.
Determine what documents and contact information is necessary to support the disaster recovery effort.
Choose the tools necessary to support the disaster recovery effort.
Determine the best way to direct the disaster recovery team.
Choose a backup strategy that will allow you to meet your recovery objectives.
Describe how upstream vendors can affect your organization’s ability to do work.
Understand how your organization can affect downstream clients’ ability to do their jobs.
Describe how the organization’s SLA impacts not only itself, but also its downstream partners.

Begin to pull together the recovery documentation.
Identify emergency situations that may occur during a recovery.
Determine what can be done if an emergency occurs during an emergency situation.
Assess the risks associated with disaster recovery.
Identify gaps in emergency recovery situations and plan accordingly.
Explain the necessity of practicing the DR plan.
Describe the different kinds of tests that can be performed.
Explain reasons for testing.
Determine the impact of testing activities.
Understand the need for change control.
Describe methods of change control.
Determine the lessons that were learned during the test disaster recovery.
Decide how to overcome the threats that were uncovered.
Use SWOT (strengths, weaknesses, opportunities, threats) analysis as an additional method of determining threats.
Plan for eliminating threats going forward.

Grading Criteria

Assignment	Pct.
Article Presentations	5%
Mid-term Exam	25%
Final Exam	25%
Paper/Presentation	10%
Group Disaster Recovery Plan Project	25%
Class Contribution & Participation	10%
Total	100%

Class contribution & participation includes amount and quality of participation in case, chapters, articles and class discussions. Quality and quantity of participation is important. You can't participate if you are not present!

Articles

Students must present two (2) high quality articles that complement class material. You must present one (1) articles before the midterm exam. This will be a short formal presentation made to the class. Expect presentations to be about 3-5 minutes in length. A written summary on the article is be to handed in with a photocopy of the first page of the article.

All written work must be done on a word processor. It shoud be double spaced, have 1 inch margins, be a 12 pitch easy to read font. Written work will be graded on content and presentation (i.e., grammar, spelling, organization, etc.). Late work is **NOT** accepted without prior approval.

Paper

Students must write and present a 5-6 page paper on a topic of interest to Disaster Recovery or Business Continuity. It could be a case study paper and presentation.

Disaster Recovery Plan

Student groups will develop a disaster recovery plan for a local business. This is a quarter long project where students will assess risks and needs for the organization if a disaster would occur. Business continuity will be included in the project.

Tentative Schedule

Week 1	Introduction
	Module 1 Erbschloe Chapter 1`
	1.1 Disaster Recovery Philosophy
	1.2 Principles of Disaster Recovery Planning
	1.3 Contingency Plan Components
	1.4 Agency Response Procedures and Continuity of Operations
	1.5 Planning Processes
	1.6 Continuity and Recovery Function
	1.7 Steps of Disaster Recovery Planning
	1.8 Role of IT and Network Management in Disaster Recovery
Week 2	Module 2 Erbschloe Chapter 2
	2.1 Developing the Disaster Recovery Plan
	2.2 Development of Plans for Recovery Actions After a Disruptive Event
	2.3 Executive Support
	2.4 DRP Leadership
	2.5 Cross Department Subcommittee
	2.6 Department Level Teams
	2.7 Relationship between IT and Network Staff with Departments
	2.8 Planning Team Skill Inventory
	2.9 DRP Team Training
	2.10 DRP Awareness Campaign
	2.11 Standards and Regulatory Bodies
Week 3	Module 3 Erbschloe Chapter 3
	3.1 Assessing Organizational Risk
	3.2 Documenting Business Processes
	3.3 Business Process Inventory
	3.4 Identifying Threats and Vulnerabilities
	3.5 Measuring and Quantifying Threats
	3.6 Risk Reports
Week 4	Module 4 Erbschloe Chapter 4
	4.1 Prioritizing systems and Functions for Recovery
	4.2 Classifying Systems
	4.3 Determination of Backup Requirements

	4.4 Emergency Destruction Procedures 4.5 Responsibility Charts 4.6 Guidelines for Determining Critical and Essential Workload 4.7 Team Member Responsibilities in Responding to an Emergency Situation 4.8 Insurance Coverage Requirements
Week 5	Midterm Exam Module 5 Erbschloe Chapter 5 5.1 Developing Plans and Procedures 5.2 Facility Index 5.3 DRP Staff 5.4 Disaster Classification 5.5 Direction, Control, and Administrative Procedures 5.6 Safety and Health Procedures 5.7 Internal and External Communication Procedures 5.8 Containment and Property Protection 5.9 Resuming and Recovering Operations 5.10 Restoring Facilities and Normalizing Operations 5.11 Development of Procedures for Off-Site Processing
Week 6	Module 6 Erbschloe Chapter 6 6.1 Disaster Recovery Relationships 6.2 DRP Partnerships 6.3 Public Service Providers 6.4 Insurance Providers 6.5 Private Service Providers 6.6 Business Arena (Partners, suppliers, customers) 6.7 Media 6.8 Stakeholders
Week 7	Module 7 Erbschloe Chapter 7 7.1 Computer Attack Procedures 7.2 Cyber attacks 7.3 Privacy Laws 7.4 Types of Attacks 7.5 Security Breach Procedures

	7.6 Working with Law Enforcement
	7.7 Economic Losses
	7.8 IT Recovery Procedures (network and systems)
	7.9 Computer Incident Response Team
Week 8	Module 8 Erbschloe Chapter 8
	8.1 Special Circumstance Procedures
	8.2 Hazardous Materials
	8.3 Art
	8.4 Historic Documents
	8.5 Perishables
	8.6 Controlled Substances
	8.7 Trade Secrets
	8.8 Animals
	8.9 Precision Equipment
	8.10 Rare Materials
Week 9	Module 9 Erbschloe Chapter 9
	9.1 Implementing DRP
	9.2 Implementation Plans
	9.3 Assigning Responsibilities
	9.4 Set Schedule
	9.5 DRP Implementation Documentation
	9.6 Internal and External Awareness Program
	9.7 Training Program
Week 10	Module 10 Erbschloe Chapter 10
	10.1 Testing and Rehearsal
	10.2 Testing Process
	10.3 Test Scenarios
	10.4 Testing Subunits
	10.5 Measuring Effectiveness
	10.6 Assessment Process
	10.7 Using the Plan in a disaster
	Final Exam
	Group Project Due