**Course Number and Name**

ISOL 533—Information Security and Risk Management

**Course Term and Delivery**

2018 Spring – IG

Asynchronous Online Course

**Course Instructor**

Dr. Jamia S. Mills

Email: Jamia.Mills@ucumberlands.edu
Office Hours: By Appointment

# Course Summary

## Course Description

This course addresses the broad topic of risk management and how risk, threats, and vulnerabilities impact information systems. Areas of instruction include how to assess and manage risk based on defining an acceptable level of risk for information systems. Elements of a business impact analysis, business continuity plan, and disaster recovery plan will also be discussed.

## Major Instructional Areas

1. Risk management basics
2. Risk assessment plan
3. Risk mitigation plan
4. Cost-benefit analysis
5. Business continuity plan
6. Disaster recovery plan

## Course Objectives

* + - 1. Explain the basic concepts of and need for risk management.
			2. Explain methods of mitigating risk by managing threats vulnerabilities, and exploits.
			3. Identify compliancy laws, standards, best practices, and policies of risk management.
			4. Describe the components of an effective organizational risk management program.
			5. Describe techniques for identifying and analyzing relevant threats, vulnerabilities, and exploits.
			6. Describe the process of performing risk assessments.
			7. Identify assets and activities to protect within an organization.
			8. Identify threats, vulnerabilities, and exploits.
			9. Identify risk mitigation security controls.
			10. Describe concepts for planning risk mitigation throughout an organization.
			11. Describe concepts for implementing a risk mitigation plan.
			12. Perform a business impact analysis.
			13. Create a business continuity plan (BCP) based on the findings of a given risk assessment for an organization.
			14. Create a disaster recovery plan (DRP) based on the findings of a given risk assessment for an organization.
			15. Create a computer incident response team (CIRT) plan for an organization.

Learning Materials and References

## Available Resources

* Gibson, Darril. *Managing Risk in Information Systems*, 2nd edition.Burlington, MA: Jones & Bartlett, 2015
* Student Lab Manual\*

\*This resource is available if your educational institution purchases the Jones & Bartlett Learning lab manual along with the courseware.

## Recommended Resources

**Web References:** Links to Web references in this document and related materials are subject to change without prior notice.

### **Books, Professional Journals**

Please use the following author’s names, book/article titles, Websites, and/or keywords to search for supplementary information to augment your learning in this subject.

* Judy Bell

*Disaster Survival Planning: A Practical Guide for Businesses*

* Thomas S. Coleman
*A Practical Guide to Risk Management*
* Kenneth L. Fulmer and Philip Jan Rothstein

*Business Continuity Planning*, A Step-by-Step Guide with Planning Forms on CD-ROM

* Ole Hanseth, et al.
*Risk, Complexity, and ICT*
* Susan Snedaker
*Business Continuity and Disaster Recovery Planning for IT Professionals*

### Other References

* **COBIT**
This URL contains information regarding COBIT from ISACA.
*http://www.isaca.org/cobit/pages/default.aspx*
* **CIPA**
This Website contains information on the Children’s Internet Protection Act from Federal Communications Commission.
[*http://www.fcc.gov/cgb/consumerfacts/cipa.html*](http://www.fcc.gov/cgb/consumerfacts/cipa.html)
* **FERPA**
This URL provides information regarding the Family Educational Rights and Privacy Act from the U.S. Department of Education.
[*http://ed.gov/policy/gen/reg/ferpa/index.html*](http://ed.gov/policy/gen/reg/ferpa/index.html)
* **FISMA**
This URL contains actual final version of the Federal Information Security Management Act.
*http://csrc.nist.gov/drivers/documents/FISMA-final.pdf*
* **GLBA**
This URL provides information regarding the Gramm-Leach-Bliley Act from the Federal Trade Commission.
[*http://www.ftc.gov/privacy/privacyinitiatives/glbact.html*](http://www.ftc.gov/privacy/privacyinitiatives/glbact.html)
* **Guide for Conducting Risk Assessments**
This URL contains NIST recommendations for conducting risk assessments for enterprise-wide risk management.
*http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf*
* **Health Information Privacy**
This URL provides information regarding the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules, from the U.S. Department of Health and Human Services.
*http://www.hhs.gov/ocr/privacy/*
* **ITIL**
This Website is an official site of for the Information Technology Infrastructure Library from AXELOS, which contains information on ITIL and provides a cohesive set of best practice, drawn from the public and private sectors internationally.
[*http://www.itil-officialsite.com/home/home.asp*](http://www.itil-officialsite.com/home/home.asp)
* **PCI**
This Website is an official site of the PCI Security Standards Council, which provides details on payment card industry security standards.
[*https://www.pcisecuritystandards.org/index.shtml*](https://www.pcisecuritystandards.org/index.shtml)
* **Risk Management Framework Overview**
This Web page provides an overview of the NIST Risk Management Framework (RMF), with links to related resources.
http://csrc.nist.gov/groups/SMA/fisma/framework.html
* **Risk Management Association**
This Website contains information on the RMA, which is a non-profit organization focusing on all aspects of risk management throughout the enterprise.
[*http://www.rmahq.org/*](http://www.rmahq.org/RMA/default.htm)*about-rma*
* **SOX**
This Website provides detailed information on the Sarbanes-Oxley Act of 2002.
*http://www.soxlaw.com/*
* **TechRepublic**
This Website contains articles, videos, pictures, white papers, webcasts, and other downloadable materials on risk management.
*http://techrepublic.com/*

**Course Outline**

Course textbook:*Managing Risk in Information Systems*, 2nd edition (Gibson, 2015)

|  |
| --- |
| **Note:**Assignments in the following table are listed when they are due. |

| Grading Category | Activity Title |
| --- | --- |
| Lesson 1: Risk Management Fundamentals, Compliance Laws, Standards, and Best Practices |
| Required Readings | * Chapter 1, “Risk Management Fundamentals”
* Chapter 3, “Managing Compliance”
 |
| Lab | Identifying Threats and Vulnerabilities in an IT Infrastructure |
| Lab | Aligning Risks, Threats, and Vulnerabilities to COBIT P09 Risk Management Controls |
| Lesson 2:Risk Management Planning |
| Required Readings | * Chapter 2, “Managing Risk: Threats, Vulnerabilities, and Exploits”
* Chapter 4, “Developing a Risk Management Plan”
 |
| Lab | Defining the Scope and Structure for an IT Risk Management Plan |
| Lesson 3: Concepts of Risk Assessment |
| Required Readings | * Chapter 5, “Defining Risk Assessment Approaches”
* Chapter 6, “Performing a Risk Assessment”
 |
| Lab | Performing a Qualitative Risk Assessment for an IT Infrastructure |
| Project  | Project Part 1 Task 1: Risk Management Plan |
| Lesson 4: Key Components of Risk Assessment |
| Required Readings | * Chapter 7, “Identifying Assets and Activities to be Protected”
* Chapter 8, “Identifying and Analyzing Threats, Vulnerabilities, and Exploits”
* Chapter 9, “Identifying and Analyzing Risk Mitigation Security Controls”
 |
| Lab | Identifying Risks, Threats, Vulnerabilities in an IT Infrastructure Using Zenmap® GUI (Nmap) and Nessus® Reports |
| Exam | Midterm Exam |
| Lesson 5: Strategies for Mitigating Risk |
| Required Readings | * Chapter 10, “Planning Risk Mitigation Throughout Your Organization”
* Chapter 11, “Turning Your Risk Assessment into a Risk Mitigation Plan”
 |
| Lab | Developing a Risk-Mitigation Plan Outline for an IT Infrastructure |
| Lesson 6: Business Impact Analysis and Continuity Planning |
| Required Readings | * Chapter 12, “Mitigating Risk with a Business Impact Analysis”
* Chapter 13, “Mitigating Risk with a Business Continuity Plan”
 |
| Lab | * Performing a Business Impact Analysis for a Mock IT Infrastructure
* Developing an Outline for a Business Continuity Plan for an IT Infrastructure
 |
| Lesson 7: Disaster Recovery, Incident Response Team, and Plan |
| Required Readings | * Chapter 14, “Mitigating Risk with a Disaster Recovery Plan”
* Chapter 15, “Mitigating Risk Assessment with a Computer Incident Response Team Plan”
 |
| Lab | Developing Disaster Recovery Backup Procedures and Recovery Instructions |
| Lab | Creating a CIRT Response Plan for a Typical IT Infrastructure |
| Lesson 8: Course Review and Final Examination |
| Required Readings | Review for Exam |
| Project | Final Submission: Risk Management Plan  |
| Exam | Final Exam |

**Evaluation and Grading**

**Evaluation Criteria**

The graded assignments will be evaluated using the following weighted categories:

| Category | Weight |
| --- | --- |
| Lab | 20 |
| Project | 24 |
| Midterm Exam | 28 |
| Final Exam | 20 |
| TOTAL | 100% |

**Grade Conversion**

The final grades will be calculated from the percentages earned in the course, as follows:

|  |  |
| --- | --- |
| **Grade** | **Percentage** |
| A | 89.5–100% |
| B | 79.5–89.4% |
| C | 69.5–79.4% |
| D | 59.5–69.4% |
| F | <59.5% |

**Course Expectations**

**Class Participation**

Students are expected to:

 1. Be fully prepared for each class session by studying the assigned reading material and preparation of the material assigned.

 2. Participate in group discussions, assignments, and panel discussions.

 3. Complete specific assignments when due and in a professional manner.

 4. Take exams when specified on the attached course schedule

**Submission of Late Work**

Students are expected to submit work on time. No late assignments will be accepted or graded unless an arrangement was made between the student and the instructor within the week the assignments were due.

**Academic Integrity**

At a Christian liberal arts University committed to the pursuit of truth and understanding, any act of academic dishonesty is especially distressing and cannot be tolerated. In general, academic dishonesty involves the abuse and misuse of information or people to gain an undeserved academic advantage or evaluation. The common forms of academic dishonesty include:

* 1. cheating - using deception in the taking of tests or the preparation of written work, using unauthorized materials, copying another person’s work with or without consent, or assisting another in such activities
	2. lying—falsifying, fabricating, or forging information in either written, spoken, or video presentations
	3. plagiarism—using the published writings, data, interpretations, or ideas of another without proper documentation

Episodes of academic dishonesty are reported to the Vice President for Academic Affairs. The potential penalty for academic dishonesty includes a failing grade on a particular assignment, a failing grade for the entire course, or charges against the student with the appropriate disciplinary body.

**Students with Disabilities**

Students who may have a disability meriting an academic accommodation should contact Dr. Tom Fish in LIB 21 to ensure that their needs are properly evaluated and that documentation is on file. **Any accommodations for disabilities must be re-certified each semester by the Academic Affairs Office before course adjustments are made by individual instructors.**

**Student Responsibilities**

1. Students are expected to login several times per week to participate in class discussions.
2. Students are expected to find out if any changes have been made in the class or assignment schedule.
3. Students are expected to be self-motivating in an online, asynchronous course.