Note:

Course content may be changed, term to term, without notice. The information below is provided as a guide for course selection and is not binding in any form, and should <u>not</u> be used to purchase course materials.

LIBERTY UNIVERSITY

COURSE SYLLABUS

BMIS 664
INFORMATION FORENSICS, COMPLIANCE AND RISK MANAGEMENT

COURSE DESCRIPTION

This course covers a diverse set of topics in information security and incident response. Risk Management domain involves the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines that ensure confidentiality, integrity and availability. The Legal, Regulations, Investigations and Compliance domains addresses computer crime laws and regulations, the investigative measures and techniques which can be used to determine if a crime has been committed and methods to gather evidence. Incident handling provides the ability to react quickly and efficiently to malicious technical threats or incidents.

RATIONALE

Competitive firms today will have the ability to proactively identify and prevent information loss. Such losses can occur by security breaches, poorly planned information systems, and by the lack of managerial guidance. To ensure a firm is compliant and prepared for information threats, risks need to be identified and prevented. Additionally, countermeasures must be implemented to mitigate and manage the potential future loss of pertinent data and information. BMIS 664 prepares the student to address such activities by examining the topics of information forensics, compliance, and risk management in greater detail.

I. PREREQUISITES

For information regarding prerequisites for this course, please refer to the Academic Course Catalog.

II. REQUIRED RESOURCE PURCHASES

Click on the following link to view the required resource(s) for the term in which you are registered: http://bookstore.mbsdirect.net/liberty.htm

III. ADDITIONAL MATERIALS FOR LEARNING

A. Computer with basic audio/video output equipment

B. Internet access (broadband recommended)

C. Microsoft Word
(Microsoft Office is available at a special discount to Liberty University students.)

IV. MEASURABLE LEARNING OUTCOMES

Upon successful completion of this course, the student will be able to:

A. Discuss the relevance of course material and the use of technology to a biblical worldview.

B. Compare risk management frameworks.

C. Conduct risk management assessments.

D. Evaluate risk management assessments.

E. Illustrate business compliance laws and regulations pertaining to information systems.

F. Support corporate computer investigations.

G. Analyze cyber forensic theories and principles.

H. Apply cyber forensic theories and principles.

I. Diagram appropriate steps to monitor and respond to security incidents.

V. COURSE REQUIREMENTS AND ASSIGNMENTS

A. Textbook readings and lecture presentations

B. Course Requirements Checklist

After reading the Course Syllabus and Student Expectations, the student will complete the related checklist found in Module/Week 1.

C. Discussion Board Forums (8)

Discussion Boards are collaborative learning experiences. Therefore, the student will write a thread containing thoughtful answers to 2 questions from the assigned module/week's textbook readings. Each answer must contain at least 250 words. No more than 4 students may answer the same question. If necessary, the student may list within his/her threads any concepts on which he/she needs further clarification. The student must also reply to at least 2 classmates' threads. Each reply must contain at least 150 words. The student may reply to a classmate's request for clarification as 1 of his/her 2 required replies.

D. Information Controls Project

Using Microsoft PowerPoint, Visio, or an alternate type of visual presentation software, the student will create a presentation intended for the controlling board of an organization that presents the advantages of implementing a biometric system. The report must be at least 5 pages (excluding the title page, diagrams, and reference page). The project must be in current APA format and must contain a minimum of 5 peer-reviewed sources.

E. Network Security Threat Project

The student will evaluate the likely threats to an organization's network and will draft an examination of these and other threats. The student must include the likely impact each would have if they were successfully implemented. The project must be a minimum of 8 pages (excluding the title page, diagrams, and reference page) and must contain at least 5 peer-reviewed sources. The project must be in current APA format.

F. Threat Interception Project

The student will evaluate the strengths and weaknesses of 3 security protocols; Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Private Communications Transport (PCT). The student must include an analysis of the threats each protocol is likely to mitigate or prevent. The project must be a minimum of 8 pages (excluding the title page, diagrams, and reference page) and must contain at least 5 peer-review sources. The project must be written in current APA format.

G. Final Project

The student will be placed in a hypothetical scenario in which an organization has been attacked and unauthorized funds have been transferred. The student must utilize all of the information gained throughout the course. The Final Project must be at least 20 pages (excluding the title page, diagrams, and the reference page). The Final Project must also contain at least 5 peer-reviewed sources and must be in current APA format.

H. Quizzes (3)

Each quiz will cover the Reading & Study material up to and including the module/week in which it is assigned. Each quiz will be open-book/open-notes, contain 12 multiple- choice questions, and have a 20-minute time limit.

I. Midterm Exam

The exam will cover the Reading & Study materials for the modules/weeks in which it is assigned. The Midterm Exam will be open-book/open-notes, contain 68 multiple-choice questions, and have a 1-hour and 30-minute time limit.

VI. COURSE GRADING AND POLICIES

A. Points

Course Requirements Checklist		10
Discussion Board Forums (8 at 25 pts ea)		200
Information Controls Project		70
Network Security Threat Project		70
Threat Interception Project		70
Final Project		240
Quizzes (3 at 60 pts ea)		180
Midterm Exam		170
	Total	1010

B. Scale

A = 940–1010 A- = 920–939 B+ = 900–919 B = 860–899 B- = 840–859
C+ = 820–839 C = 780–819 C- = 760–779 F = 0–759

C. Disability Assistance

Students with a documented disability may contact Liberty University Online's Office of Disability Academic Support (ODAS) at LUOODAS@liberty.edu to make arrangements for academic accommodations. Further information can be found at www.liberty.edu/disabilitysupport.

LIBERTY UNIVERSITY

COURSE SCHEDULE

BMIS 664

Textbook: Pfleeger & Pfleeger, *Analyzing Computer Security* (2012).

MODULE/ WEEK	READING & STUDY	ASSIGNMENTS	POINTS
1	Pfleeger & Pfleeger: chs. 1–2 1 presentation 1 website	Course Requirements Checklist Class Introductions DB Forum 1	10 0 25
2	Pfleeger & Pfleeger: chs. 3–5 1 presentation 1 website	DB Forum 2 Information Controls Project Quiz 1	25 70 60
3	Pfleeger & Pfleeger: chs. 6–7 1 presentation	DB Forum 3 Network Security Threat Project	25 70
4	Pfleeger & Pfleeger: chs. 8–10 1 presentation 1 website	DB Forum 4 Midterm Exam	25 170
5	Pfleeger & Pfleeger: chs. 11–12 1 presentation	DB Forum 5 Threat Interception Project Quiz 2	25 70 60
6	Pfleeger & Pfleeger: chs. 13–14 2 presentations	DB Forum 6	25
7	Pfleeger & Pfleeger: chs. 15–16 1 presentation	DB Forum 7 Quiz 3	25 60
8	Pfleeger & Pfleeger: chs. 17–18 1 presentation	DB Forum 8 Final Project	25 240
		TOTAL	**1010**

DB = Discussion Board

NOTE: Module/Week 1 begins on Monday and ends at 11:59 p.m. (ET) on Friday.
Modules/Weeks 2-8 begin on Saturday and end at 11:59 p.m. (ET) on Friday.