IS305T
Managing Risk in Information Systems
[Onsite and Online]

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.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IT260T Networking Application Services and Security or equivalent

Credit hours: 4

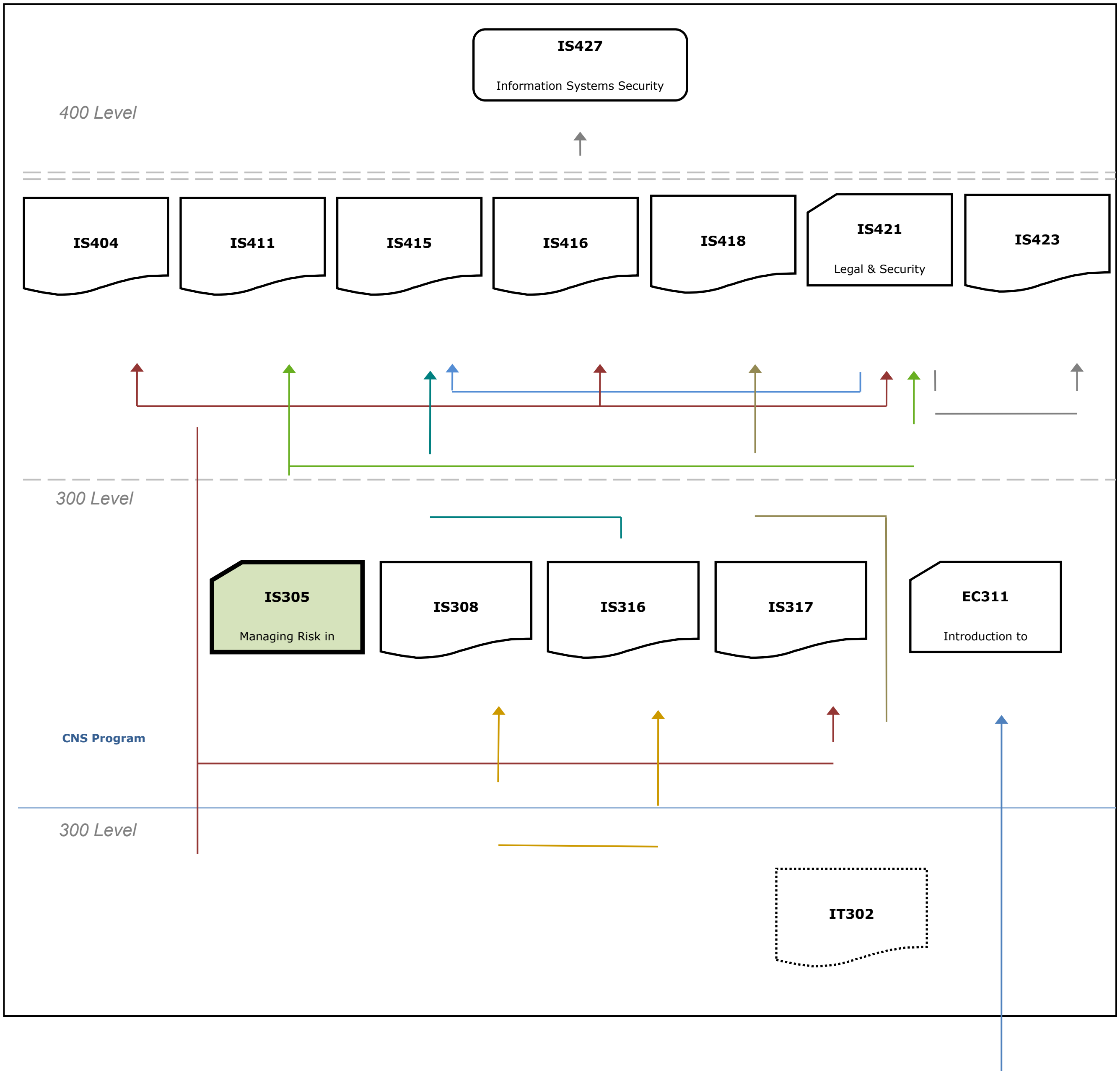
Contact hours: 60 (36 Theory Hours, 24 Lab Hours)

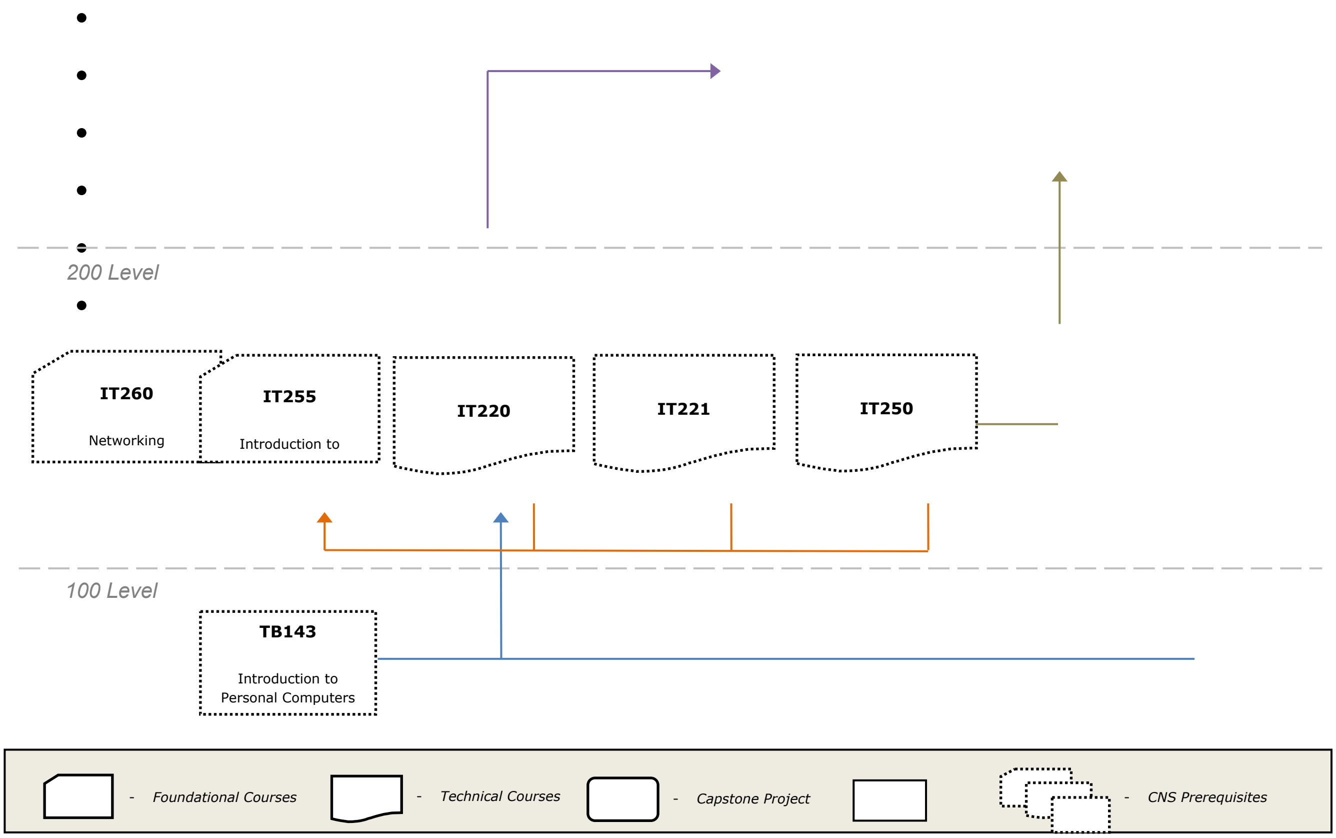
Where Does This Course Belong?

This course is required for the Bachelor of Science in Information Systems Security program. This program covers the following core areas:

- Foundational Courses
- Technical Courses
- BSISS Project

The following diagram demonstrates how this course fits in the program:




200 Level
IT260
Networking
IT255
Introduction to
IT220
IT221
IT250
100 Level
TB143
Introduction to
Personal Computers
- Foundational Courses
- Technical Courses
- Capstone Project
- CNS Prerequisites

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 and benefit analysis
5. Business continuity plan
6. Disaster recovery plan

Course Objectives

1. Explain the basic concepts of and need for risk management.
2. Identify compliancy laws, standards, best practices, and policies of risk management.
3. Describe the components of an effective organizational risk management program.
4. Describe techniques for identifying relevant threats, vulnerabilities, and exploits.
5. Identify risk mitigation security controls.
6. Describe concepts for implementing risk mitigation throughout an organization.
7. Perform a business impact analysis for a provided scenario.

8. Create a business continuity plan (BCP) based on the findings of a given risk assessment for an organization.

9. Create a disaster recovery plan (DRP) based on the findings of a given risk assessment for an organization.

10. Create a Computer Incident Response Team (CIRT) plan for an organization in a given scenario.

SCANS Objectives

SCANS is an acronym for Secretary’s Commission on Achieving Necessary Skills. The committee, appointed by the National Secretary of Labor in 1990, created a list of skills and competencies that continue to be a valuable resource for individuals developing their careers in a high-tech job market. For more information on the SCANS objectives, visit The U.S. Department of Labor Employment and Training Administration: www.doleta.gov.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Gibson, Darril. *Managing Risk in Information Systems.* 1st ed. Sudbury, MA: Jones & Bartlett, 2011.	■		
Companion CD-IS305	■		
Printed IS305 Student Lab Manual	■		

Recommended Resources

Books, Professional Journals

Please use the following author's names, book/article titles and/or keywords to search in the ITT Tech Virtual Library for supplementary information to augment your learning in this subject:

- Ole Hanseth, et al., *Risk, Complexity, and ICT*.

Search in:

Books > Books 24x7

Periodicals . EbscoHost

Other References

- COBIT

  This URL contains information regarding COBIT from the ISACA.

  http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981 (accessed on April 28, 2010)

- CIPA

  This Website contains information on the Children's Internet Protection Act from Federal Communications Commission.

  http://www.fcc.gov/cgb/consumerfacts/cipa.html (accessed on April 28, 2010)

- DIACAP

  Information regarding the Department of Defense Information Assurance Certification and Accreditation Process from the Defense Information Systems Agency

  http://iase.disa.mil/diacap/ (accessed on April 28, 2010)

- 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 (accessed on April 28, 2010)

- FISMA

  This URL contains actual final version of the Federal Information Security Management Act.

  http://csrc.nist.gov/drivers/documents/FISMA-final.pdf (accessed on April 28, 2010)

- GLBA

This URL provides information regarding the Gramm-Leach Bliley Act from the Federal Trade Commission.

http://www.ftc.gov/privacy/privacyinitiatives/glbact.html (accessed on April 28, 2010)

- Health Information Privacy

  This URL provides information regarding HIPPA from the U.S. Department of Health and Human Services.

  http://www.hhs.gov/ocr/privacy/ (accessed on April 28, 2010)

- ITIL

  This Website is an official site of for the Information Technology Infrastructure Library from the OGC 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 (accessed on April 28, 2010)

- PCI

  This Website is an official site of the PCI Security Standards Council which provides details on security standards.

  https://www.pcisecuritystandards.org/index.shtml (accessed on April 28, 2010)

- 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/RMA/default.htm (accessed on April 28, 2010)

- Risk Management Guide for Information Technology Systems

  This URL contains NIST recommendations for the U.S. Department of Commerce on Risk Management for Information Technology Systems.

  http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (accessed on April 28, 2010)

- SOX

  This Website provides detailed information on the Sarbanes-Oxley Act of 2002.

  http://www.soxlaw.com/ (accessed on April 28, 2010)

- TechRepublic

  This Website contains articles, videos, pictures, white papers, webcasts, and downloads material on risk management.

  http://techrepublic.com.com/ (accessed on April 28, 2010)

NOTE: All links are subject to change without prior notice.

Information Search

Use the following keywords to search for additional online resources that may be used for supporting your work on the course assignments:

COBIT

CIPA

DIACAP

FERPA

FISMA

GLBA

Health Information, Privacy

ITIL

PCI

Risk Management Association

Risk Management Guide for Information Technology Systems

SOX

TechRepublic

Course Plan

Instructional Methods

This course is designed to promote learner-centered activities and support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and group learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook ▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards the points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment components every day

Course Outline

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
1	Risk Management Fundamentals	*Managing Risk in Information Systems*: ▪ Chapter 1 ▪ Chapter 2	Quiz	1.1	An open book quiz over the assigned reading of Unit 1.	1
			Lab	1.2	Identifying Threats and Vulnerabilities	2
			Assignment	1.3	Application of risk management techniques	3
Course Project and associated deliverables are introduced.						
2	Compliance Laws, Standards, and Best Practices	*Managing Risk in Information Systems*: ▪ Chapter 3	Quiz	2.1	Quiz 2.1	1
			Lab	2.2	COBIT Framework	2
			Assignment	2.3	PCI DSS and the seven domains	3
3	Risk Management Planning	*Managing Risk in Information Systems*: ▪ Chapter 4	Quiz	3.1	Quiz 3.1	1
			Lab	3.2	Risk management scope/boundaries	2
			Discussion	3.3	Risk Management Process	5
4	Concepts of Risk Assessment	*Managing Risk in Information Systems*: ▪ Chapter 5 ▪ Chapter 6	Quiz	4.1	Quiz 4.1	1
			Lab	4.2	Risk Assessment Pre-Planning	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
			Assignment	4.3	Risk Assessment Approaches	3
			Project	4.4	Risk Management Plan Project Part 1	5
5	Key Components of Risk Assessment	*Managing Risk in Information Systems*: ▪ Chapter 7 ▪ Chapter 8 ▪ Chapter 9	Quiz	5.1	Quiz 5.1	1
			Lab	5.2	Perform a Risk Assessment	2
			Discussion	5.3	Risk Assessment and Risk Mitigation control	5
6	Strategies for Mitigating Risk	*Managing Risk in Information Systems*: ▪ Chapter 10 ▪ Chapter 11	Quiz	6.1	Quiz 6.1	1
			Lab	6.2	Risk Mitigation	2
			Project	6.3	Risk Assessment Plan	3
7	Business Impact Analysis	*Managing Risk in Information Systems*: ▪ Chapter 12	Quiz	7.1	Quiz 7.1	1
			Lab	7.2	Business impact analysis	2
			Project	7.3	Risk Mitigation Plan	3

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
8	Business Continuity Planning	*Managing Risk in Information Systems*: ▪ Chapter 13	Quiz	8.1	Quiz 8.1	1
			Lab	8.2	Reviewing business continuing planning techniques	2
			Project	8.3	Risk Management Plan Project Part 2	5
9	Disaster Recovery Planning	*Managing Risk in Information Systems*: ▪ Chapter 14	Quiz	9.1	Quiz 9.1	1
			Lab	9.2	Disaster recovery techniques	2
			Project	9.3	Conducting a business continuity plan	3
10	Structuring Computer Incident Response Team and Plan	*Managing Risk in Information Systems*: ▪ Chapter 15	Quiz	10.1	Quiz 10.1	1
			Lab	10.2	CIRT planning techniques	2
			Project	10.3	Disaster Recovery Plan	2
11	Course Review and Final Exam	N/A	Project	11.1	Project: Risk Management Plan	10
			Exam	11.2	Final Exam	20

Evaluation and Grading

Evaluation Criteria

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

Category	Weight
Discussion	10
Assignment	9
Lab	20
Project	31
Quiz	10
Exam	20
TOTAL	**100%**

Grade Conversion

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

Grade	Percentage	Credit
A	90–100%	4.0
B+	85–89%	3.5
B	80–84%	3.0
C+	75–79%	2.5
C	70–74%	2.0
D+	65–69%	1.5

D	60–64%	1.0
F	<60%	0.0

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage. For more information on the academic honesty policies, refer to the Student Handbook.

(End of Syllabus)