

**ITT Technical Institute**  
**IS3110**  
**Risk Management in Information**  
**Technology Security**  
**Onsite Course**

**SYLLABUS**

---

**Credit hours:** 4.5

**Contact/Instructional hours:** 60 (30 Theory Hours, 30 Lab Hours)

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

Prerequisite: NT2580 Introduction to Information Security or equivalent

**Course Description:**

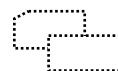
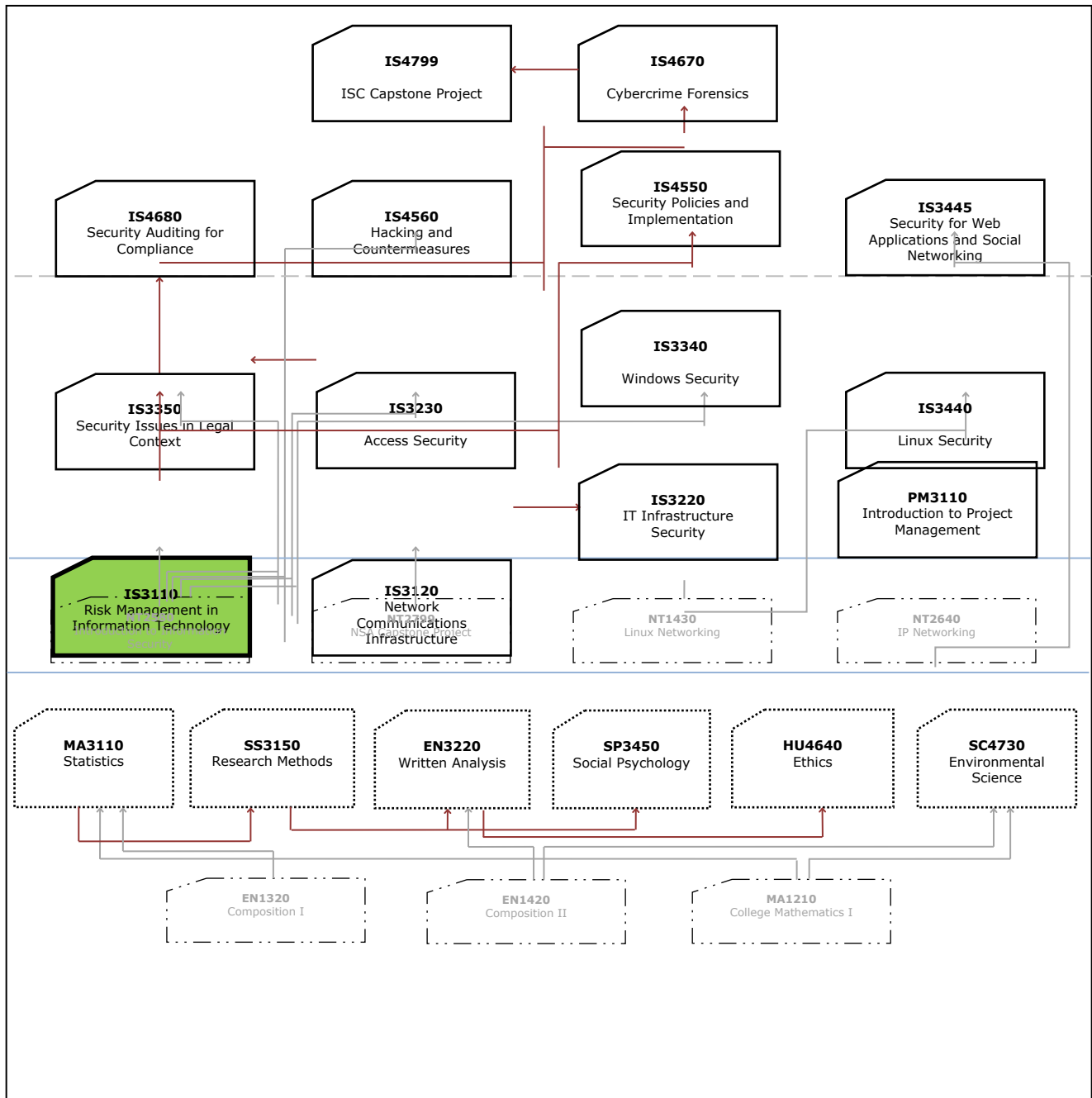
This course addresses how risk, threats and vulnerabilities impact information systems in the context of risk management. Topics include methods of assessing, analyzing and managing risks, defining an acceptable level of risk for information systems, and identifying elements of a business impact analysis, a business continuity plan and a disaster recovery plan.

## 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:



# Course Summary

---

## Course Description

This course addresses how risk, threats and vulnerabilities impact information systems in the context of risk management. Topics include methods of assessing, analyzing and managing risks, defining an acceptable level of risk for information systems, and identifying elements of a business impact analysis, a business continuity plan and a disaster recovery plan.

## 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.

## 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. <i>Managing Risk in Information Systems</i> . 1 <sup>st</sup> ed. Sudbury, MA: Jones & Bartlett, 2011.	■		
Printed IS3110 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
<ul style="list-style-type: none"> <li>▪ Do take a proactive learning approach</li> <li>▪ Do share your thoughts on critical issues and potential problem solutions</li> <li>▪ Do plan your course work in advance</li> <li>▪ Do explore a variety of learning resources in addition to the textbook</li> <li>▪ Do offer relevant examples from your experience</li> <li>▪ Do make an effort to understand different points of view</li> <li>▪ Do connect concepts explored in this course to real-life professional situations and your own experiences</li> </ul>	<ul style="list-style-type: none"> <li>▪ Don't assume there is only one correct answer to a question</li> <li>▪ Don't be afraid to share your perspective on the issues analyzed in the course</li> <li>▪ Don't be negative towards the points of view that are different from yours</li> <li>▪ Don't underestimate the impact of collaboration on your learning</li> <li>▪ Don't limit your course experience to reading the textbook</li> <li>▪ Don't postpone your work on the course deliverables – work on small assignment components every day</li> </ul>

## Course Outline

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
1	Risk Management Fundamentals	<i>Managing Risk in Information Systems:</i> <ul style="list-style-type: none"> <li>▪ Chapter 1</li> <li>▪ Chapter 2</li> </ul>	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
<b>Course Project and associated deliverables are introduced.</b>						
2	Compliance Laws, Standards, and Best Practices	<i>Managing Risk in Information Systems:</i> <ul style="list-style-type: none"> <li>▪ Chapter 3</li> </ul>	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	<i>Managing Risk in Information Systems:</i> <ul style="list-style-type: none"> <li>▪ Chapter 4</li> </ul>	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	<i>Managing Risk in Information Systems:</i> <ul style="list-style-type: none"> <li>▪ Chapter 5</li> <li>▪ Chapter 6</li> </ul>	Quiz	4.1	Quiz 4.1	1
			Lab	4.2	Risk Assessment Pre-Planning	2
			Assignment	4.3	Risk Assessment Approaches	3
			Project	4.4	Risk Management Plan Project Part 1†	5



Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation
						(% of all graded work)
5	Key Components of Risk Assessment	<i>Managing Risk in Information Systems:</i> <ul style="list-style-type: none"> <li>▪ Chapter 7</li> <li>▪ Chapter 8</li> <li>▪ Chapter 9</li> </ul>	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	<i>Managing Risk in Information Systems:</i> <ul style="list-style-type: none"> <li>▪ Chapter 10</li> <li>▪ Chapter 11</li> </ul>	Quiz	6.1	Quiz 6.1	1
			Lab	6.2	Risk Mitigation	2
			Project	6.3	Risk Assessment Plan†	3
7	Business Impact Analysis	<i>Managing Risk in Information Systems:</i> <ul style="list-style-type: none"> <li>▪ Chapter 12</li> </ul>	Quiz	7.1	Quiz 7.1	1
			Lab	7.2	Business impact analysis	2
			Project	7.3	Risk Mitigation Plan†	3
8	Business Continuity Planning	<i>Managing Risk in Information Systems:</i> <ul style="list-style-type: none"> <li>▪ Chapter 13</li> </ul>	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

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation
						(% of all graded work)
9	Disaster Recovery Planning	<i>Managing Risk in Information Systems:</i> ▪ 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	<i>Managing Risk in Information Systems:</i> ▪ 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

† Candidate for ePortfolio

## 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
<b>TOTAL</b>	<b>100%</b>

### 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)