

## Course Overview

During this course, you will learn how to identify common information security risk analysis methodologies, their characteristics, pros and cons, and application. You will examine the sources of risk, as well as external malicious attackers, intentional and accidental attacks by internal users as well as threats from environmental and structural sources of risk. You will also identify vulnerabilities in hardware, software, locations, and procedures that provide an opening to attackers and create risk to organizations. You will demonstrate risk assessment techniques through hands-on labs to apply fundamental risk management strategies and approaches for mitigating risk.

## Course Competencies

(Read Only)

To successfully complete this course, you will be expected to:

- 1 Analyze the range and level of threat that exists in cyberspace.
- 2 Analyze the role that security policy plays in risk identification and mitigation.
- 3 Analyze information technology systems to discover vulnerabilities that introduce risk to the organization.
- 4 Apply risk mitigation strategies and actions that reduce risk to organization due to identified information technology systems vulnerabilities.
- 5 Analyze the how administrative, technical and physical controls work together to manage risk in an organization.
- 6 Communicate effectively to a range of professional and technical audiences.

## Course Prerequisites

Prerequisite(s): IAS5025.

## Syllabus >> Course Materials

### Required

The materials listed below are required to complete the learning activities in this course.

### Integrated Materials

Many of your required books are available via the VitalSource Bookshelf link in the courseroom, located in your Course Tools. Registered learners in a Resource Kit program can access these materials using the courseroom link on the Friday before the course start date. Some materials are available only in hard-copy format or by using an access code. For these materials, you will receive an email with further instructions for access. Visit the [Course Materials](#) page on Campus for more information.

## Book

Gibson, D. (2015). *Lab manual to accompany Managing Risk in Information Systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning. ISBN: 9781284192612.

Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning. ISBN: 9781284055955.

## Library

The following required readings are provided in the Capella University Library or linked directly in this course. To find specific readings by journal or book title, use [Journal and Book Locator](#). Refer to the [Journal and Book Locator library guide](#) to learn how to use this tool.

- Bertino, E. (2012). [Synthesis lectures on data management: Data protection from insider threats](#). San Rafael, CA: Morgan & Claypool.

## External Resource

Please note that URLs change frequently. While the URLs were current when this course was designed, some may no longer be valid. If you cannot access a specific link, contact your instructor for an alternative URL. Permissions for the following links have been either granted or deemed appropriate for educational use at the time of course publication.

- Digit. (2016). [Hacking websites & apps and howto secure your customers data \[Video\]](#). | [Transcript](#) Retrieved from [https://www.youtube.com/watch?v=mdWe\\_Nupy40](https://www.youtube.com/watch?v=mdWe_Nupy40)
- Gadia, S. (n.d.). [Cloud computing risk assessment: A case study](#). Retrieved from <https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Cloud-Computing-Risk-Assessment-A-Case-Study.aspx>
- ISACA. (n.d.). [COBIT case study: IT risk management in a bank](#). Retrieved from <https://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-IT-Risk-Management-in-a-Bank.aspx>
- ISACA. (n.d.). [Risk IT case study: Risk IT framework for IT risk management: A case study of National Stock Exchange of India Limited](#). Retrieved from <http://www.isaca.org/Knowledge-Center/cobit/Pages/Risk-IT-Case-Study-Risk-IT-Framework-for-IT-Risk-Management-A-Case-Study-of-National-Stock-Exchange-of-India-Limited.aspx>
- JBSwebcasts. (2012). [JBS – Webinar – Introduction to SARMA and the overview of US security risk management \(Ed Jopeck\).\[Video\]](#). | [Transcript](#) Retrieved from <http://www.youtube.com/watch?v=RBGV5-5LuCc>
- Jones & Bartlett Learning. (2012). [Lab 5 Nessus vulnerability scan report](#). Retrieved from [http://d2jw81rkebrcvk.cloudfront.net/assetsnav2/Managing\\_Risk\\_in\\_Information\\_Systems\\_2e\\_Lab\\_Access\\_43010\\_3/Risk\\_manual/Lab%20%20Nessus%20Vulnerability%20Scan%20Report.pdf](http://d2jw81rkebrcvk.cloudfront.net/assetsnav2/Managing_Risk_in_Information_Systems_2e_Lab_Access_43010_3/Risk_manual/Lab%20%20Nessus%20Vulnerability%20Scan%20Report.pdf)
- Jones & Bartlett Learning. (2012). [Lab 5 Nmap scan report](#). Retrieved from [http://d2jw81rkebrcvk.cloudfront.net/assetsnav2/Managing\\_Risk\\_in\\_Information\\_Systems\\_2e\\_Lab\\_Access\\_43010\\_3/Risk\\_manual/Lab%20%20Nmap%20Scan%20Report.pdf](http://d2jw81rkebrcvk.cloudfront.net/assetsnav2/Managing_Risk_in_Information_Systems_2e_Lab_Access_43010_3/Risk_manual/Lab%20%20Nmap%20Scan%20Report.pdf)
- Lisbon, S., & Rice, E. (2017). [Case study: Information security risk assessment for a small healthcare clinic using the security risk assessment tool provided by HealthIT.gov \[PDF\]](#). Retrieved from [http://www.micsymposium.org/mics\\_2017\\_proceedings/docs/MICS\\_2017\\_paper\\_7.pdf](http://www.micsymposium.org/mics_2017_proceedings/docs/MICS_2017_paper_7.pdf)
- Mitre. (n.d.). [Common vulnerabilities and exposures](#). Retrieved from <http://cve.mitre.org>
- Mitre. (n.d.). [Risk impact assessment and prioritization](#). Retrieved from <http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization>
- Nehemiah Security. (2017). [Introduction to security risk management \(SRM series, part 1\).\[Video\]](#). | [Transcript](#) Retrieved from <https://www.youtube.com/watch?v=w6jN3g5NDg4>
- NIST. (2017). [Security and privacy controls for information systems and organizations: Initial public draft \[PDF\]](#). Retrieved from <https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf>
- Nmap. (n.d.). [Downloading Nmap](#). Retrieved from <https://nmap.org/download.html>
- Nmap. (n.d.). [Interpreting scan results](#). Retrieved from <https://nmap.org/book/zenmap-results.html>
- Northern Territory Government of Australia. (2013). [The risk management process \[PDF\]](#). Retrieved from [https://web.archive.org/web/20130418005540/http://www.education.nt.gov.au/\\_\\_data/assets/pdf\\_file/0011/4106/risk\\_management\\_process.pdf](https://web.archive.org/web/20130418005540/http://www.education.nt.gov.au/__data/assets/pdf_file/0011/4106/risk_management_process.pdf)
- RSA Conference. (2011). [RSA Conference 2011 - security metrics: A beginner's guide - Caroline Wong \[Video\]](#). | [Transcript](#) Retrieved from <http://www.youtube.com/watch?v=dFsbqGJ3qEY>
- RSA Conference. (2011). [RSA conference 2011 – risk and resilience: Considerations for security risk assessment \[Video\]](#). | [Transcript](#) Retrieved from [http://www.youtube.com/watch?v=NmX3gJY\\_EJU](http://www.youtube.com/watch?v=NmX3gJY_EJU)
- RSA Conference. (2012). [Webcast: Security awareness — maybe it's not about the users \[Video\]](#). | [Transcript](#) Retrieved from <http://www.youtube.com/watch?v=nyrMW3Ylgal>
- RSA Conference. (2013). [Webcast: Mitigating the top human risks \[Video\]](#). | [Transcript](#) Retrieved from <http://www.youtube.com/watch?v=g7TNgBH6tQI>
- SANS Institute. (2016). [SANS Reading room: Case studies](#). Retrieved from <https://www.sans.org/reading-room/whitepapers/casestudies>
- Stebbins-Wheelock, E. J., & Turgeon, A. (2018). [Guide to risk assessment and response \[PDF\]](#). Retrieved from [https://www.uvm.edu/sites/default/files/UVM-Risk-Management-and-Safety/Guide\\_to\\_Risk\\_Opportunity\\_Assessment\\_Response.pdf](https://www.uvm.edu/sites/default/files/UVM-Risk-Management-and-Safety/Guide_to_Risk_Opportunity_Assessment_Response.pdf)
- Stoneburner, G., Goguen, A., & Feringa, A. (2002). [Risk management guide for information technology systems \[PDF\]](#). Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf>
- Whitmore, W. (2013). [Security compliance: Using online resources to meet the HIPAA training and awareness requirements \[Video\]](#). | [Transcript](#) Retrieved from <http://www.youtube.com/watch?v=hu8eOpZuMf0>
- Workplace Answers. (2014). [Information security training: Mitigating risk through awareness \[Webinar\]](#). | [Transcript](#) Retrieved from <http://www.youtube.com/watch?v=yLuGy0VIMWg>

## Suggested

The following materials are recommended to provide you with a better understanding of the topics in this course. These materials are not required to complete the course, but they are aligned to course activities and assessments and are highly recommended for your use.

## Optional

The following optional materials are offered to provide you with a better understanding of the topics in this course. These materials are not required to complete the course.

## Library

The following optional Skillsoft resources are available via the Capella University Library.

- Humphreys, E. (2016). [Implementing the ISO/IEC 27001 ISMS standard \(2nd ed.\)](#). Norwood, MA: Artech House.
- Lachance, D. (2015). [CISSP: Assessing risk \[Video\]](#). Skillsoft Ireland.
- Lachance, D. (2015). [CISSP: Software security risk analysis and mitigation \[Video\]](#). Skillsoft Ireland.
- Lacoste, R. (2017). [Security+: Security awareness training \[Video\]](#). Skillsoft Ireland.
- Lacoste, R. (n.d.). [CompTIA Security+ SY0-501: Policies, plans, and procedures \[Tutorial\]](#). Skillsoft.
- Shannon, M. (2016). [CISA: Compliance vs. substantive testing \[Video\]](#). Skillsoft Ireland.
- Shannon, M. (2017). [CISM: Available InfoSec governance frameworks \[Video\]](#). Skillsoft Ireland.
- Shannon, M. (n.d.). [Information risk management, part 1 \[Tutorial\]](#). Skillsoft.
- Shannon, M. (n.d.). [Information risk management, part 2 \[Tutorial\]](#). Skillsoft.
- Skillsoft. (n.d.). [CISM: Information security program development and management, part 3 \[Tutorial\]](#).
- Skillsoft. (n.d.). [CISSP: Risk management \[Tutorial\]](#).
- Skillsoft. (n.d.). [CISSP: Security operations part 1 \[Tutorial\]](#).
- Skillsoft. (n.d.). [CISSP: Security operations, part 3 \[Tutorial\]](#).
- Skillsoft. (n.d.). [CISSP: Security principles, governance, and guidelines \[Tutorial\]](#).
- Skillsoft. (n.d.). [IT security for end users: IT security fundamentals \[Tutorial\]](#).
- Welton, T. (2015). [IT security for end users: End user role in IT security \[Video\]](#). Skillsoft Ireland.
- Wheeler, E. (2011). [Security risk management: Building an information security risk management program from the ground up](#). Waltham, MA: Syngress.

## Projects

### Project >> IT Risk Management Plan

#### Project Overview

## Project Overview

This course project will provide you with an opportunity to demonstrate your proficiency in the course competencies by synthesizing and applying your learning into an IT risk management plan for a given scenario or for an organizational setting of your choice. Understand that this project is a work in progress throughout the quarter. You are urged and expected to continually enrich the quality of your final IT risk management plan. This course will present opportunities to enhance your IT risk management plan as you move through the quarter. Demonstrating your ability to recognize and identify these opportunities is a valuable skill and talent. The final IT risk management plan will apply the [IT Risk Management Plan Template](#) provided in this course that includes the following elements:

- Plan Header and Table of Contents.
- Executive Summary.
  - Summary of Findings.
  - Prioritization of Risk Assessment Elements.
  - Risk Assessment Summary and Impact.
  - Recommendations.
- Plan Objectives.
- Plan Scope.
- Roles and Responsibilities.
- Information from the following assignments:
  - Unit 2: Course Project: Draft IT Risk Management Plan.
  - Unit 3: LAB: Outlining an IT Risk Management Plan.
  - Unit 4: LAB: Performing a Qualitative Risk Assessment for an IT Infrastructure.
  - Unit 7: LAB: Developing a Risk Mitigation Plan Outline for an IT Infrastructure.
  - Unit 8: Course Project: Final IT Risk Management Plan.
- Findings and Recommendations.

- Summary Statements.

## Project Topic

Choose from one of the following two options for your IT risk management plan.

### Option 1

Apply the information provided in the assignment labs for the health care IT structure servicing patients with life threatening conditions.

### Option 2

Apply the information from an organization of your choice. You must gain instructor approval for your choice and the following criteria must be met:

- You must have access to the organization for the 10-week duration of this course.
- You must have access at minimum an overview level of the IT infrastructure of the organization.

## Unit 1 >> What Is Risk?

### Introduction

#### This week you will:

- Identify threats and vulnerabilities that create risk in an IT infrastructure.
- Study federal laws and the effect these laws have on IT security policies, standards and guidelines.

What is a risk? A risk is a probability that a loss could happen. Losses happen when a vulnerability is exposed by a threat (Gibson, 2015). It is important for a business to discern between minor and severe risks in order to allocate funds optimally to protect the organization, its customers and clients, and its personnel. Once risks are categorized, decisions can be made as to whether the risk will be mitigated, avoided, shared, transferred, or accepted. In addition, companies are required to understand and comply with a number of laws and regulations that apply to their industry. An understanding of the relevant laws and the compliance requirements is essential in order to avoid costly fines, penalties, and even jail time for noncompliance. Understanding these laws also provides a foundation for understanding and assessing risk associated with potential threats and vulnerabilities that may exploit an IT infrastructure.

These resources can help you learn more about risk.

Use the textbook to read:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 1, "Risk Management Fundamentals," pages 2–27.
  - Chapter 3, "Maintaining Compliance," pages 57–83.

Use the Internet to study:

- Nehemiah Security. (2017). [Introduction to security risk management \(SRM series, part 1\) \[Video\]](https://www.youtube.com/watch?v=w6jN3g5NDg4). Retrieved from <https://www.youtube.com/watch?v=w6jN3g5NDg4>

### Reference

Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.

### Learning Activities

#### u01d1 - Threats and Vulnerabilities Creating IT Infrastructure Risk

In this discussion, we examine the seven domains of IT Infrastructure and their related potential threats and vulnerabilities. Generally speaking, these threats and vulnerabilities are composed of two types—those caused by people (such as embezzlement and fraud), and those caused by technology (such as phishing, pharming, and phreaking).

## Discussion Question

List the seven domains of IT infrastructure. Select one domain answer the following questions.

1. What is possible threat to this domain?
2. How could this threat exploit potential vulnerabilities or weaknesses in this domain?
3. How could the resulting exploit impact an organization?

Your initial discussion post must be submitted by 11:59 PM Thursday.

## Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

### Course Resources

Graduate Discussion Participation Scoring Guide

### u01d1 - Learning Components

- Assess the different types of attacks and their characteristics.
- Use style and vocabulary generally appropriate to the message and intended audience.

### u01a1 - LAB: Identifying Threats and Vulnerabilities in an IT Infrastructure

## Overview

Systematically searching for risk across an entire IT system is a daunting task. However, by dividing the IT environment into seven domains and searching for threats and vulnerabilities in each domain, the process becomes more organized. The seven domains of an IT infrastructure are wide area network (WAN), local area network (LAN), system and application, remote access, user, and workstation. Using these seven domains, it is possible to organize responsibilities, roles, and accountabilities for managing and mitigating risk. In the first lab for this course, you will organize and map a set of risks, vulnerabilities, and threats within the seven domains as they pertain to a specific scenario or organizational context. You can use the assessment worksheet included with the lab as a study guide, but you will not submit it with your lab report.

## Instructions

1. Complete Lab 1 in your lab manual, *Lab Manual to Accompany Managing Risk in Information Systems*.
2. Complete the IT Infrastructure Threats and Vulnerabilities table provided in the resources for this assignment.
3. Insert your completed IT Infrastructure Threats and Vulnerabilities table in your lab report.
4. Submit your lab report for Lab 1 to the assignment for this unit. Be sure your report meets all of the criteria for this assignment.

## Assignment Criteria

Your assignment must meet these criteria. Please refer to the scoring guide for this assignment.

- Identify basic threats, vulnerabilities, and risks across the seven domains of IT infrastructure.
- Align the identified risks, threats, and vulnerabilities to each of the seven domains of a typical IT infrastructure.
- Describe how identified risks can impact each of the seven domains of an IT infrastructure.
- Determine which of the domains of an IT infrastructure is most impacted by an identified risk, threat, or vulnerability.
- Use style and vocabulary generally appropriate to the message and intended audience.

## Assignment Requirements

- **Lab Report:** Lab report with elements described in the assignment criteria. This report is considered a professional document and should therefore follow the corresponding academic and professional guidelines, including single-spaced paragraphs.
- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Resources and citations are formatted according to APA (6th edition) style and formatting.

- **Font and font size:** Times New Roman, 12 point.

## Course Resources

IT Infrastructure Threats and Vulnerabilities [DOCX]

[Academic and Professional Document Guidelines \[PDF\]](#)

### u01s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Capella Library to study:

- Bertino, E. (2012). [Synthesis lectures on data management: Data protection from insider threats](#). San Rafael, CA: Morgan & Claypool.
- Skillsoft. (n.d.). [CISSP: Security operations part 1 \[Tutorial\]](#).

### u01s1 - Learning Components

- Assess the different types of attacks and their characteristics.

## Unit 2 >> Risk Management and Compliance

### Introduction

#### This week you will:

- Assess risk threats, vulnerabilities, and exploits.
- Analyze the impact of a data breach and the impact it had on an organization in a case study.
- Apply federal compliance laws to the analysis of a case study where a data breach occurred.
- Draft an IT risk management plan to begin your course project.

You will add to your IT risk management plan while you work through the course assignments and will submit your final IT risk management plan to complete your course project in Unit 8.

In order to manage information system security risks, the source of the risk must be understood. Threats, vulnerabilities, and vulnerability/threat pairs are those sources. Organizations that have experienced a data breach have risk associated from threats and vulnerabilities that exploit an IT infrastructure. Understanding what occurred within an organization that has experienced a data breach can help strengthen risk assessment and mitigation in the future. Understanding risk assessment and mitigation is essential for IT risk management and developing an IT risk management plan.

These resources can help you learn more about risk threats, vulnerabilities, and exploits.

Use the textbook to read:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 2, "Managing Risk: Threats, Vulnerabilities, and Exploits," pages 29–54.
  - Chapter 4, "Developing a Risk Management Plan," pages 85–109.

Use the Internet to access case studies. You will use one of the case studies in the discussion for this unit.

- SANS Institute. (2016). [SANS Reading room: Case studies](#). Retrieved from <https://www.sans.org/reading-room/whitepapers/casestudies>

### Learning Activities

#### u02d1 - Learning About Risk Assessment Through Case Studies

The business impact of a data breach can be devastating to an organization. Reading and evaluating case studies regarding organizations that have experienced a data breach are useful in understanding how to more effectively perform a risk assessment.

## Discussion Question

Select one of the case studies related to a data breach at the SANS reading room.

- Briefly summarize the data breach case.
- What cybersecurity regulations or laws were relevant in this case?
- What threats or vulnerabilities were overlooked in the case you reviewed?
- What security controls should the company have had in place to avoid the breach?
- What steps did the organization take to improve security after the breach?
- What was the business impact of the breach?

Your initial discussion post must be submitted by 11:59 PM Thursday.

## Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide with or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

### Course Resources

Graduate Discussion Participation Scoring Guide

[SANS Reading Room: Case Studies](#)

u02d1 - Learning Components

- Evaluate internal risk with respect to technology and people related to a specific scenario.
- Use style and vocabulary generally appropriate to the message and intended audience.
- Evaluate the level of risk to Internet facing organizations.

**u02a1 - Course Project: Draft IT Risk Management Plan**

## Assignment Overview

This course includes a course project for the creation of an IT risk management plan that includes an outline for a risk mitigation plan. Review the course project description to see which assignments will be incorporated into your final IT risk management plan. For this assignment, you will download the IT Risk Management Plan template, review the template to become familiar with each of the elements of the plan, and confirm with your instructor if you are using the scenario provided in the labs or an organizational setting of your choice.

## Choose Your Project

You may use the health care institution example provided in the scenario found in your labs manual for your course project, or one of your choosing. If you are using another organization check with your instructor to confirm you have an appropriate organizational setting for your course project and resulting IT risk management plan.

## Assignment Instructions

1. Download the IT Risk Management Plan Template, linked in the Resources.
2. Review the template and save the file as *[Your Name]* IT Risk Management Plan.
3. Complete the following information in the header:
  - Project Name: Use "Health Care Institution" or the name of the approved project you chose.
  - Learner Name:
  - Course Name:
  - Date:
4. Write the plan objectives, plan scope, and the roles and responsibilities for your IT risk management plan using the template provided with this assignment.
5. Information from the following assignments will be incorporated into your final IT Risk Management Plan.
  - Unit 2: Course Project: Draft IT Risk Management Plan.
  - Unit 3: LAB: Outlining an IT Risk Management Plan.
  - Unit 4: LAB: Performing a Qualitative Risk Assessment for an IT Infrastructure.
  - Unit 7: LAB: Developing a Risk Mitigation Plan Outline for an IT Infrastructure.
  - Unit 8: Course Project: Final IT Risk Management Plan.

## Assignment Criteria

Your assignment must meet these criteria. Please refer to the scoring guide for this assignment.

- Write objectives for an IT risk management plan.
- Write a scope statement for an IT risk management plan.
- Write the roles and responsibilities for an IT risk management plan.
- Use style and vocabulary generally appropriate to the message and intended audience.

## Assignment Requirements

- **IT Risk Management Plan:** IT Risk Management Plan draft aligned with the IT Risk Management Plan template. The IT Risk Management Plan is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Resources and citations are formatted according to APA (6th edition) style and formatting.
- **Font and font size:** Times New Roman, 12 point.

### Course Resources

IT Risk Management Plan Template [DOCX]

[Academic and Professional Document Guidelines \[PDF\]](#)

### u02s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Capella Library to study:

- Wheeler, E. (2011). [Security risk management: Building an information security risk management program from the ground up](#). Waltham, MA: Syngress.
- Skillsoft. (n.d.). [CISM: Information security program development and management, part 3 \[Tutorial\]](#).
- Skillsoft. (n.d.). [CISSP: Security principles, governance, and guidelines \[Tutorial\]](#).

### u02s1 - Learning Components

- Evaluate internal risk with respect to technology and people related to a specific scenario.
- Evaluate the level of risk to Internet facing organizations.

## Unit 3 >> Developing a Risk Management Plan

### Introduction

#### This week you will:

- Outline and develop the elements of a risk management plan.
- Study the process for conducting risk management.
- Develop a risk assessment table that describes risk as probability multiplied by impact for identified threats and vulnerabilities.
- Add the risk assessment table to your IT risk management plan.

Risk management follows a general process that planning for risk management, risk identification, risk assessment, responding to risk, and monitoring risk. While there are variations of the risk management process, each of these main steps of risk management are followed. The IT risk management plan is a document that records how an organization plans to manage risk. Reflected in the document are the steps of risk identification, risk assessment, responding to risk, and monitoring risk.

This resource can help you learn more about the elements of a risk management plan and the process for risk management.

Use the textbook to read:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Review Chapter 4, "Developing a Risk Management Plan," pages 850–109.
  - Chapter 6, "Performing Risk Assessment," pages 138–163.

## Learning Activities

### u03d1 - The Sections of an IT Risk Management Plan

In your lab this week, you will be creating an outline for an IT risk management plan. There are core elements of an IT risk management plan, and there are seven domains in a typical IT infrastructure. The IT plan must address all of the domains of an IT infrastructure. Once the IT risk management plan is complete, key stakeholders and decision makers will choose to accept, defer, or modify the risks.

## Discussion Questions

Select one of the following case studies, linked in the Resources, related to IT risk management that is of interest to you:

1. COBIT Case Study: IT Risk Management in a Bank.
2. A Case Study of National Stock Exchange of India Limited.
3. Cloud Computing Risk Assessment: A Case Study.

Describe and discuss each of the following important elements of the risk management plan case study.

- The plan objectives.
- The scope of the plan.
- The roles and responsibilities of the team members.
- Findings and recommendations.

Your initial discussion post must be submitted by 11:59 PM Thursday.

## Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

### Course Resources

Graduate Discussion Participation Scoring Guide

[Cloud Computing Risk Assessment: A Case Study](#)

[COBIT Case Study: IT Risk Management in a Bank](#)

[Risk IT Case Study: Risk IT Framework for IT Risk Management: A Case Study of National Stock Exchange of India Limited](#)

### u03d1 - Learning Components

- Develop an IT risk management plan.
- Use style and vocabulary generally appropriate to the message and intended audience.
- Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.

### u03a1 - LAB: Defining the Scope and Structure for an IT Risk Management Plan

## Assignment Overview

Risk management requires understanding the threats that exist, how impactful each threat is, and the actions that can be taken to mitigate risks. This lab covers information technology (IT) risk management within the seven domains of an IT infrastructure. During this lab, you will review the risk management process. Then, you will expand upon the scope for your IT Risk Management Plan by further defining the risk using the Risk Equals Probability Times Impact table provided with this assignment. This table sets the stage for your risk assessment, which is covered in the next unit. You can use the assessment worksheet included with the lab as a study guide, but you will not submit it with your lab report.

## Assignment Instructions

1. Complete **Steps 1–10, 12, and 13 only** for Lab 3 (pages 18 and 19) in your lab manual. Follow the instructions provided.
2. Complete the Risk Equals Probability Times Impact table found in the Resources for this assignment.

3. Add the Risk Equals Probability Times Impact table to your draft IT Risk Management Plan.
4. Upload *both* the Lab 3 Report and your updated draft IT Risk Management Plan to this assignment.

## Assignment Criteria

Your assignment must meet these criteria, please refer to the scoring guide for this assignment.

- Describe the process for IT risk management.
- List the risk, threats, and vulnerabilities for each domain of an IT infrastructure.
- Describe the impact risk has for each identified threat.
- Relate identified risks, threats, and vulnerabilities and the potential impact of each in an IT risk management plan for a given organizational context.
- Use style and vocabulary generally appropriate to the message and intended audience.

## Assignment Requirements

- **Lab Report:** Lab report with elements described in the assignment criteria. This report is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **IT Risk Management Plan:** IT Risk Management Plan draft aligned with the IT Risk Management Plan template. The IT Risk Management Plan is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Resources and citations are formatted according to APA (6th edition) style and formatting.
- **Font and font size:** Times New Roman, 12 point.

### Course Resources

Risk Equals Probability Times Impact Table [XLSX]

[Academic and Professional Document Guidelines \[PDF\]](#)

[Guide to Risk Assessment and Response](#)

[The Risk Management Process](#)

## u03s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Internet to study:

- Stoneburner, G., Goguen, A., & Feringa, A. (2002). [Risk management guide for information technology systems \[PDF\]](#). Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf>

Use the Capella Library to study:

- Lachance, D. (2015). [CISSP: Assessing risk \[Video\]](#). Skillsoft Ireland.
- Shannon, M. (n.d.). [Information risk management, part 1 \[Tutorial\]](#). Skillsoft.
- Skillsoft. (n.d.). [CISSP: Risk management \[Tutorial\]](#).

### u03s1 - Learning Components

- Analyze the role that policies and procedures play in selection of specific tools and controls.
- Develop a strategy for measuring and monitoring the effectiveness of an existing security management program.
- Evaluate the commonly used risk analysis methodologies.

## Unit 4 >> Defining Risk Assessment Approaches

### Introduction

This week you will:

- Analyze risk assessment and approaches to risk assessment.
- Examine the similarities and differences between quantitative and qualitative risk assessments.
- Conduct a qualitative risk assessment.
- Insert the qualitative risk assessment into your IT risk management plan.

Risk assessment is a key risk management activity that provides the foundation for risk mitigation. Risk assessment involves identification and prioritization of risk and the identification of countermeasures to the risk, and the best methods for risk mitigation. There are two general types of risk assessment, quantitative and qualitative. Quantitative risk assessment involves numerical data and dollar values, and qualitative risk assessment involves determining the probability and impact of a risk through expert opinion. Each of these methods has a purpose and a place for managing risk, depending upon the context of the risk and the organization.

This resource can help you learn more about risk assessment.

Read from the textbook:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 5, "Defining Risk Assessment Approaches," pages 112–136.

## Learning Activities

### u04d1 - Information Technology Risk Assessment: Quantitative or Qualitative?

IT departments perform risk assessments to determine risks that are most probable and of the highest impact. A risk assessment provides a prioritization of identified risks so that leaders can make plans to manage high-impact risks and perhaps accept the lower-impact risks. Once risks are identified and prioritized, the optimal controls are assessed and selected for risk mitigation. There are two general types of risk assessments: qualitative and quantitative. The qualitative assessment uses plain language to describe risk levels rather than numeric results from formulas. The qualitative assessment looks at the probability of risk and the impact of the risk. On the other hand, a quantitative risk assessment will use specific formulas such as annual loss expectancy (ALE), single loss expectancy (SLE), and the annual rate of occurrence (ARO).

## Discussion Question

Discuss the difference in the types of results received between the quantitative and qualitative approach to risk assessment. Discuss the pros and cons of each approach.

Consider the quantitative and qualitative risk assessment methodologies with respect to **one** of the following scenarios and provide a conclusion about what each method would provide and which method might produce the most helpful results for the scenario:

1. A five-physician family health general practice business which has recently implemented electronic health records (EHR).
2. A well-established large retail firm that operates globally and sells products in brick and mortar stores as well as online. The organization has what they consider to be strong security controls in place.
3. A publicly traded bank that does business in over 35 states nationwide, providing standard banking services, loan services, and investment advisory services.

Your initial discussion post must be submitted by 11:59 PM Thursday.

## Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide with or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

### Course Resources

Graduate Discussion Participation Scoring Guide

### u04d1 - Learning Components

- Analyze security controls and tools that are available to mitigate risk.
- Use style and vocabulary generally appropriate to the message and intended audience.
- Analyze the advantages and disadvantages of various risk assessment methodologies.

### u04a1 - LAB: Performing a Qualitative Risk Assessment for an IT Infrastructure

## Overview

In order to assess risk, vulnerabilities, threats, and risks must first be identified. Once they are identified, each one will be assessed in terms of the probability of that risk occurring and the impact of that risk. Risk equals likelihood multiplied by impact. Risks cannot be mitigated until they are prioritized based on this formula. In this lab, you will define the purpose of a risk assessment, use the qualitative method for assessing risk, and label risks as either critical, major, or minor. You will perform this risk assessment within the scenario or organizational context that you have used in previous assessments. When you have completed prioritizing the risks, you will write an executive summary that summarizes the risk assessment findings, the overall impact, and your recommendations to mitigate areas of noncompliance. You can use the assessment worksheet included with the lab as a study guide, but you will not submit it with your lab report.

## Instructions

1. Complete Lab 4: Performing a Qualitative Risk Assessment for an IT Infrastructure in the lab manual.
2. Complete the IT Infrastructure Qualitative Risk Assessment table provided in the resources for this assignment.
3. Insert your completed IT Infrastructure Qualitative Risk Assessment into your draft IT Risk Management Plan.
4. Insert the executive summary from your Lab Report into your draft IT Risk Management Plan.
5. Upload *both* the Lab 4 Report and your updated draft IT Risk Management Plan to the assignment for this unit.

## Assignment Criteria

Your assignment must meet these criteria. Please refer to the scoring guide for this assignment.

1. Define the purpose and objectives of an IT risk assessment.
2. Align the identified vulnerabilities, threats, and risks to an IT risk assessment that incorporates the seven domains of a typical IT infrastructure.
3. Classify identified vulnerabilities, threats, and risks based on a qualitative risk assessment template.
4. Prioritize classified vulnerabilities, threats, and risks based on the defined qualitative risk assessment scale.
5. Write an executive summary that addresses the risk assessment results and risk assessment impact, and provide recommendations to mitigate areas of noncompliance.
6. Use style and vocabulary generally appropriate to the message and intended audience.

## Assignment Requirements

- **Lab Report:** Lab report with elements described in the assignment criteria. This report is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **IT Risk Management Plan:** IT Risk Management Plan draft aligned with the IT Risk Management Plan template. The IT Risk Management Plan is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Resources and citations are formatted according to APA (6th edition) style and formatting.
- **Font and font size:** Times New Roman, 12 point.

### Course Resources

IT Infrastructure Qualitative Assessment [DOCX]

[Academic and Professional Document Guidelines \[PDF\]](#)

## u04s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Internet to study:

- Digit. (2016). [Hacking websites & apps and howto secure your customers data \[Video\] | Transcript](#). Retrieved from [https://www.youtube.com/watch?v=mdWe\\_Nupy40](https://www.youtube.com/watch?v=mdWe_Nupy40)

Use the Capella Library to study:

- Humphreys, E. (2016). [Implementing the ISO/IEC 27001 ISMS standard \(2nd ed.\)](#). Norwood, MA: Artech House.
- Shannon, M. (n.d.). [Information risk management, part 2 \[Tutorial\]](#). Skillssoft.
- Skillssoft. (n.d.). [CISSP: Security principles, governance, and guidelines \[Tutorial\]](#).

## u04s1 - Learning Components

- Analyze security controls and tools that are available to mitigate risk.

- Analyze the advantages and disadvantages of various risk assessment methodologies.

## Unit 5 >> Protect Against Risk Events

### Introduction

#### This week you will:

- Identify assets in the risk management process and risk assessment.
- Identify different types of assets an organization may have, and describe threats that may exist for those assets.

Identification of assets allows an organization to understand how risk occurs when threats exploit vulnerabilities associated with its assets. For example, hardware, software, and data are all assets of an organization that can be vulnerable to threats if a viable risk management plan is not in place. These assets can be exploited if they are not first identified and inventoried as assets, and second protected through risk management planning and risk mitigation. An organization that applies asset identification and inventory for mitigation will also have a solid foundation for business impact planning, business continuity planning, disaster recovery planning, business insurance liability planning, and asset replacement insurance planning. These activities occur within an organization to mitigate risk by reducing threats that can exploit the organization's assets.

This resource can help you learn more about identifying assets for a risk assessment.

Read from the textbook:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 7, "Identifying Assets and Activities to be Protected," pages 166–193.

### Learning Activities

#### u05d1 - Identifying Critical Assets for Risk Assessment – 1

A thorough inventory of all that needs to be protected in an organization is needed before a risk assessment can begin. There are many types of assets and this first discussion will address a subset of valuable assets that might exist. Assets can be tangible like hardware and software, can be data related, and can also relate to system function and processes. Services can be assets as well. Elements of an organization's business continuity plan and data recovery plan are also considered assets that need protection.

### Discussion Question

Think about the organization you currently work for or an organization you have worked for in the past. Identify what you feel are the most critical assets in each of these categories:

1. Information assets.
2. Software.
3. Physical assets.
4. Hardware.
5. Services that a computer system depends on.
6. People.
7. Intangible intellectual property.

Describe at least two critical threats that can exist for each class of asset. You may discuss the threat under each critical asset that you list.

Your initial discussion post must be submitted by 11:59 PM Thursday.

### Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide with or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

Course Resources

Graduate Discussion Participation Scoring Guide

## u05d1 - Learning Components

- Use style and vocabulary generally appropriate to the message and intended audience.
- Evaluate the level of risk to Internet facing organizations.

## u05d2 - Identifying Critical Assets for Risk Assessment – 2

### Discussion Question

In the same work environment discussed in Discussion 1, discuss the following other classes of activities and assets and related threats in terms of which are most critical for the specific organization:

1. System access and availability.
2. System functions.
3. Data warehousing and data mining.
4. Facilities and supplies for maintaining business operations (Business Continuity Plan and Disaster Recovery Plan).

As in Discussion 1, describe at least two threats related to each activity/asset you list as critical. The threats can be described under each asset/activity.

Your initial discussion post must be submitted by 11:59 PM Thursday.

### Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide with or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

#### Course Resources

Graduate Discussion Participation Scoring Guide

## u05d2 - Learning Components

- Develop an IT risk management plan.
- Use style and vocabulary generally appropriate to the message and intended audience.
- Evaluate the level of risk to Internet facing organizations.

## u05s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Internet to study:

- JBSwebcasts. (2012). [JBS – Webinar – Introduction to SARMA and the overview of US security risk management \(Ed Jopeck\).\[Video\]](http://www.youtube.com/watch?v=RBGV5-5LuCc) | [Transcript](#). Retrieved from <http://www.youtube.com/watch?v=RBGV5-5LuCc>
- RSA Conference. (2011). [RSA conference 2011 – risk and resilience: Considerations for security risk assessment \[Video\]](http://www.youtube.com/watch?v=NmX3gJY_EJU) | [Transcript](#). Retrieved from [http://www.youtube.com/watch?v=NmX3gJY\\_EJU](http://www.youtube.com/watch?v=NmX3gJY_EJU)
- RSA Conference. (2011). [RSA Conference 2011 - security metrics: A beginner's guide - Caroline Wong.\[Video\]](http://www.youtube.com/watch?v=dFsbqGJ3qEY) | [Transcript](#). Retrieved from <http://www.youtube.com/watch?v=dFsbqGJ3qEY>

Use the Capella Library to study:

- Shannon, M. (2017). [CISM: Available InfoSec governance frameworks \[Video\]](#). Skillsoft Ireland.

## u05s1 - Learning Components

- Analyze the role that policies and procedures play in selection of specific tools and controls.
- Develop an IT risk management plan.
- Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.
- Develop an IT risk mitigation plan.

### Introduction

#### This week you will:

- Identify vulnerabilities that may allow threats that can potentially exploit an organization.
- Apply the NMAP and Nessus vulnerability scan tools to identify network vulnerabilities.
- Analyze the effectiveness of the application of risk mitigation tools.

Information learned from the identification of threats and vulnerabilities provide the foundation for the risk assessment and the resulting risk management and risk mitigation plans. NMAP and Nessus are two software tools used to conduct IT network analysis for vulnerabilities to threats that lead to risk. Also, hundreds, if not thousands, of known threats and vulnerabilities are cataloged on sites such as the Common Vulnerabilities and Exposures database provided by the Mitre Corporation, an organization driven to solving the world's problems in the domain of cybersecurity as well as other domains important to safety and stability (Mitre, n.d.). Identification of threats and vulnerabilities provides input for the identification and analysis of risk mitigation controls.

The following resources will help you learn more about identifying threats and vulnerabilities.

Use the textbook to read:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 8, "Identifying and Analyzing Threats, Vulnerabilities, and Exploits," pages 194–250.

Use the Internet to study:

- Mitre. (n.d.). [Risk impact assessment and prioritization](http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization). Retrieved from <http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization>

Reference

Mitre. (n.d.). Common vulnerabilities and exposures. Retrieved from <http://cve.mitre.org>

### Learning Activities

#### u06d1 - Risk Mitigation and the Organization

As outlined in NIST Special Publication 800-30, linked in the Resources, the foundation for the development of an effective configuration management program contains both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal of such a system is to help organizations to better manage IT-related mission risks, which constitute the net negative impact of the exercise of vulnerabilities, considering both the probability and the impact of their occurrence. Thus, as the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level, risk management is the critical driver in any effective configuration management program.

### Discussion Questions

In your post, select and refer to an organization with which you are familiar or can research in substantial detail regarding the tools that are used to mitigate risk in the organization's information security.

- What tools are used by the organization in mitigating risk?
- Why were the tools chosen?
- Do the tools chosen comply with the organization's security policies with regard to risk mitigation?
- From the perspective of the organization's INFOSEC personnel, are the tools likely to be successful in risk mitigation? Why?

Your initial discussion post must be submitted by 11:59 PM Thursday.

Reference

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems [PDF]. Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf>

### Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide with or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

## Graduate Discussion Participation Scoring Guide

[Risk Management Guide for Information Technology Systems](#)

## u06d1 - Learning Components

- Analyze security controls and tools that are available to mitigate risk.
- Use style and vocabulary generally appropriate to the message and intended audience.
- Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.

**u06a1 - LAB: Identifying Risks, Threats, and Vulnerabilities in an IT Infrastructure Using Nmap and Nessus Reports**

## Overview

Vulnerability scanners test vulnerabilities to see if they exist but also to see if they have been properly closed after a patch or control has been put in place. There are two widely used vulnerability scanners, Nmap and Nessus, which produce scan reports. By using these reports, you can identify operating systems, services, hosts, open ports, and applications that are vulnerable in an organization.

- In Part 1 of this lab, you will have an opportunity to review and analyze Nessus and Nmap reports to determine the vulnerabilities that exist in a system. You will then use the mitre.org website to search for common vulnerabilities and exposures (CVE) listings that you identify in the vulnerability scan reports that you analyze. You can use the assessment worksheet included with the lab as a study guide, but you will not submit it with your lab report.
- In Part 2 of this lab, you will download the Nmap software and use a test site provided by Nmap to run a number of scans.

## Part 1: Lab 5

Complete Lab 5 in the lab manual. **Note:** The Lab 5 Nmap Scan Report and the Lab 5 Nessus Vulnerability Scan Report listed in the Lab 5 hands-on instructions are linked in the Resources for this assignment.

## Part 2: Nmap Test Network Scan

Go to this [Downloading Nmap](#) site and download the latest stable release of Nmap for the operating system that you use. You will want to download the self-installer. For example, if you are using a Windows operating system you will look for a link that looks similar to this: **Latest stable release self-installer: nmap-7.70-setup.exe**. **Note:** The version number may have changed, but the description of the download will be similar.

To do this test:

1. Click the setup.exe file that downloads and follow the instructions on the screen, leaving all default settings selected. **Note:** Once Nmap is installed, you should see an icon on your desktop that you can use to run Nmap.
2. Open Nmap.
3. Type **scanme.nmap.org** in the *Target* field.
4. Select **Quick scan** from the *Profile* drop down list.
5. Click **Scan**. A list appears of the ports, the state of each port, and the service.
6. Take a screenshot of the scan results and copy it at the bottom of the Word document used for Part 1.
7. Run a Regular scan and one other scan of your choice, taking screenshots of each and adding to the Word document.

Underneath your screenshots write a brief summary of your experience using Nmap and discuss briefly what the scan results showed you.

You can learn more about the Nmap interface and interpreting scans at [Interpreting Scan Results](#).

## Instructions

1. Complete Lab 5 in the lab manual as directed in the Part 1 instructions.
2. Write your lab report as directed in the lab.
3. Complete the Nmap test network scan for Part 2.
4. Add the screenshots from Part 2 to your lab report.
5. Upload the lab report with the test network scan screenshot to the assignment for this unit.

## Assignment Criteria

Your assignment must meet these criteria. Please refer to the scoring guide for this assignment.

- Review an Nmap network discover and port scanning report and a Nessus software vulnerability report.
- Identify minor, major, and critical software vulnerabilities from the Nessus vulnerability assessment scan report.

- Identify operating systems, applications, services, hosts, and open ports on devices from the Nmap scan report.
- Use the Common Vulnerabilities and Exposures (CVE) online listing of software vulnerabilities and conduct searches on this site and describe the search results.
- Download, install, and use Nmap to run a variety of vulnerability scans.
- Use style and vocabulary generally appropriate to the message and intended audience.

## Assignment Requirements

- **Lab Report:** Lab report with elements described in the assignment criteria including screenshots from the Nmap test network vulnerability scan. This report is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Resources and citations are formatted according to APA (6th edition) style and formatting.
- **Length of paper:** At least 5 pages, excluding the references page.
- **Font and font size:** Times New Roman, 12 point.

### Course Resources

[Lab 5 Nmap Scan Report](#)

[Lab 5 Nessus Vulnerability Scan Report](#)

[Interpreting Scan Results](#)

[Academic and Professional Document Guidelines \[PDF\]](#)

[Risk Impact Assessment and Prioritization](#)

[Downloading Nmap](#)

### u06s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Internet to study:

- RSA Conference. (2012). [Webcast: Security awareness — maybe it's not about the users \[Video\] | Transcript](#). Retrieved from <http://www.youtube.com/watch?v=nyrMW3Ylgal>

Use the Capella Library to study:

- Lachance, D. (2015). [CISSP: Software security risk analysis and mitigation \[Video\]](#). Skillsoft Ireland.

### u06s1 - Learning Components

- Assess the different types of attacks and their characteristics.
- Analyze security controls and tools that are available to mitigate risk.
- Evaluate the level of risk to Internet facing organizations.

## Unit 7 >> Identifying and Analyzing Risk Mitigation Controls

### Introduction

#### This week you will:

- Study the National Institute of Standards and Technology (NIST) families of control for risk mitigation.
- Develop an outline for a risk mitigation plan that will be the basis for the risk mitigation section of your IT risk management plan.
- Develop the risk mitigation section of your IT risk management plan.

Risk assessment and mitigation includes the identification and prioritization of risks, threats, and vulnerabilities and their countermeasures. Included with a risk mitigation plan is the considerations of cost and impact the countermeasures have to the identified risks, threats, and vulnerabilities, and the IT infrastructure of an organization. The

risk mitigation plan documents the prioritization of the risks, threats, and vulnerabilities, and their countermeasures and the tactics for implementation, including identification of critical risks, short-term remediation steps for critical risks, long-term remediation for major and minor risks, ongoing risk mitigation steps, and potential cost estimates.

These resources can help you learn more about controls for risk mitigation and developing a risk mitigation plan.

Use the textbook to read:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 9, "Identifying and Analyzing Risk Mitigation Security Controls," pages 224–250.

Use the Internet to review:

- NIST. (2017). [Security and privacy controls for information systems and organizations: Initial public draft \[PDF\]](https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf). Retrieved from <https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf>
  - Appendix E.

## Learning Activities

### u07d1 - Identifying the NIST Control Families and Related Controls

The National Institute of Standards and Technology (NIST) have special publications that are invaluable to IT professionals working in the United States. These publications provide security best practices for IT security professionals. In regards to risk mitigation, NIST published SP 800-53 revision 5 in August of 2017. This publication offers guidance on over 200 security controls that reside within 20 control families developed by NIST. These controls handle many existing security issues. When determining risk mitigation strategies and deciding on which controls are best suited across the seven domains of an IT infrastructure, SP 800-53 provides a detailed description of the controls along with supporting references on how the controls should be implemented. Appendix E of SP 800-53 version 5 provides the detailed documentation for the controls in each of the families.

## Discussion Questions

Review the NIST control families and select a control family that you want to review. Access the NIST SP800-53 version 5 document. Go to Appendix E and locate the control family that you want to examine and select two specific controls under that family. Please note that the control families are designated by a two-letter acronym. Those acronyms are shown on page 251 of your textbook. For example, Access Control family is designated by AC.

1. Describe the control.
2. Discuss the supplemental guidance that is provided for each control.
3. If there are enhancements for that control, describe one of the enhancements.

Your initial discussion post must be submitted by 11:59 PM Thursday.

### Reference

NIST. (2017). [Security and privacy controls for information systems and organizations: Initial public draft \[PDF\]](https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf). Retrieved from <https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf>

## Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

### Course Resources

#### Graduate Discussion Participation Scoring Guide

[Security and Privacy Controls for Information Systems and Organizations: Initial Public Draft](#)

### u07d1 - Learning Components

- Analyze security controls and tools that are available to mitigate risk.
- Use style and vocabulary generally appropriate to the message and intended audience.
- Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.

## Overview

Risk management requires understanding the threats that exist, how impactful each threat is, and the actions that can be taken to mitigate risks. Another part of risk management is monitoring for risk once controls are in place. This lab will cover information technology (IT) risk management within the seven domains of an IT infrastructure. During this lab, you will state the purpose and scope for an IT risk mitigation plan that includes the seven domains of an IT infrastructure and will incorporate the risks, threats, and vulnerabilities to the plan. You can use the assessment worksheet included with the lab as a study guide, but you will not submit it with your lab report.

## Instructions

1. Complete Lab 6 in the lab manual.
2. Complete the following. Both are provided in the Resources.
  - o IT Risk Assessment Countermeasures table.
  - o IT Risk Assessment Countermeasure Considerations table.
3. Add the IT Risk Assessment Countermeasures and the IT Risk Assessment Countermeasure Considerations tables to your draft IT Risk Management Plan.
4. Update the Risk Mitigation Section of your IT Risk Management Plan.
5. Upload *both* the Lab 6 Report and your updated draft IT Risk Management Plan to the assignment for this unit.

## Assignment Criteria

Your assignment must meet these criteria. Please refer to the scoring guide for this assignment.

- Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.
- Align the major parts of an IT risk mitigation plan in each of the seven domains of a typical IT infrastructure.
- Define the tactical risk-mitigation steps required to remediate the identified vulnerabilities, threats, and risks typically found in the seven domains of an IT infrastructure.
- Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.
- Create an outline for an IT risk mitigation plan incorporating the seven domains of an IT infrastructure.
- Use style and vocabulary generally appropriate to the message and intended audience.

## Assignment Requirements

- **Lab Report:** Lab report with elements described in the assignment criteria. This report is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **IT Risk Management Plan:** IT Risk Management Plan draft aligned with the IT Risk Management Plan template. The IT Risk Management Plan is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Resources and citations are formatted according to APA (6th edition) style and formatting.
- **Font and font size:** Times New Roman, 12 point.

### Course Resources

IT Risk Assessment Countermeasures [DOCX]

IT Risk Assessment Countermeasure Considerations [DOCX]

[Academic and Professional Document Guidelines \[PDF\]](#)

## u07s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Internet to study:

- Workplace Answers. (2014). [Information security training: Mitigating risk through awareness \[Webinar\] | Transcript](http://www.youtube.com/watch?v=yLuGy0VIMWg). Retrieved from http://www.youtube.com/watch?v=yLuGy0VIMWg

Use the Capella Library to study:

- Lacoste, R. (2017). [Security+: Security awareness training \[Video\]](#). Skillssoft Ireland.

- Skillsoft. (n.d.). [CISSP: Security operations, part 3 \[Tutorial\]](#).

## u07s1 - Learning Components

- Assess the different types of attacks and their characteristics.
- Analyze security controls and tools that are available to mitigate risk.
- Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.

## Unit 8 >> Planning Risk Mitigation Throughout the Organization

### Introduction

#### This week you will:

- Examine business impact analysis in risk assessment and cost-benefit analysis when evaluating a control.
- Complete your final IT risk management plan and submit it for your final course project assignment.

Business impact assessment and cost-benefit analysis are activities that occur in the risk assessment process that help an organization decide what actions to take to mitigate risk. Information from these activities inform the risk mitigation and risk management plans for an organization. Completion of an IT risk management plan may consider these and other risk management and risk assessment activities for the identification, assessment, mitigation, and control of risk in an IT infrastructure.

The following resource will help you learn more about organizational planning for risk mitigation and developing a risk mitigation plan.

Use the textbook to read:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 10, "Planning Risk Mitigation Throughout Your Organization," pages 252–279.
  - Chapter 11, "Turning Your Risk Assessment Into a Risk Mitigation Plan," pages 282–310.

### Learning Activities

#### u08d1 - Business Impact Analysis in Risk Assessment

Both a broad and a narrow approach must be taken toward risk management. While it is true that systems and process risks must be identified, it is equally important that security awareness and training is implemented. Risk management must emerge from business needs, meaning that the risks that are managed are the ones that potentially can affect the organization. It is not justifiable to manage risks outside of that scope. There are many steps to implementing a sound risk management program. High-level phases of risk assessment include identifying critical assets, identifying the scope of risk management, identifying risk across the seven domains of IT infrastructure, identifying relevant legal and compliance requirements, knowing the impact of noncompliance to regulations, identifying risk mitigation, and performing a cost-benefit analysis.

### Discussion Question Part 1

From your study activities in this course and cursory research, analyze and discuss the role of a business impact analysis (BIA) in the risk assessment process. Consider the following in your response:

- Direct and indirect costs.
- Maximum acceptable outage (MAO).
- Minimum tolerable period of disruption (MTPD).

### Discussion Question Part 2

One of the most important factors in a BIA is to identify an organization's mission-critical business functions and the related critical success factors (CSFs). A CSF is any factor required to perform the business mission and required for the organization to be successful. There are specific processes that lead to achieving the CSFs.

Think about the organization that you work for. For this specific organization:

- Identify at least four CSFs and indicate why each is a CSF for this organization.
- Describe the processes that support each of those CSFs.
- Identify the critical IT and human resources required for each process that supports the CSF.

What is the importance of identifying these critical resources in performing the business impact analysis?

Your initial discussion post must be submitted by 11:59 PM Thursday.

## Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide with or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

### Course Resources

Graduate Discussion Participation Scoring Guide

### u08d1 - Learning Components

- Analyze security controls and tools that are available to mitigate risk.
- Use style and vocabulary generally appropriate to the message and intended audience.
- Analyze the advantages and disadvantages of various risk assessment methodologies.

### u08a1 - Course Project: Final IT Risk Management Plan

## Assignment Overview

As you progressed through the course, you used the IT Risk Management Plan template that includes an outline for a risk mitigation plan. You have chosen an organization for your plan, and in Unit 2 you wrote the plan objectives, plan scope, and roles and responsibilities for your IT Risk Management Plan. You have also incorporated results from your lab assignments in Units 3, 4, 6, and 7. Now, in Unit 8, you will make sure you have compiled all of these elements into a single, cohesive document.

## Assignment Instructions

1. Compile all of the required elements created in previous units into a single, cohesive document. Make sure you label each section with an appropriate heading.
2. If you are using the scenario in the labs use "Health Care Institution" as the Project Name, and if you are using another organization provide the project name of your choice.
3. Include the plan objectives, plan scope, and roles and responsibilities for your IT Risk Management Plan that you wrote for Unit 2.
4. Incorporate the following into your final IT Risk Management Plan:
  - Assignment 2: Course Project: Draft IT Risk Management Plan.
  - Assignment 3: LAB: Outlining an IT Risk Management Plan.
  - Assignment 4: LAB: Performing a Qualitative Risk Assessment for an IT Infrastructure.
  - Assignment 7: LAB: Developing a Risk Mitigation Plan Outline for an IT Infrastructure.
5. Add a summary at the end of the IT Risk Management Plan
6. Provide a list of references at the end of the paper.

## Assignment Criteria

Your assignment must meet these criteria. Please refer to the scoring guide for this assignment.

- Write objectives for an IT risk management plan.
- Write a scope statement for an IT risk management plan.
- Write the roles and responsibilities for an IT risk management plan.
- Develop tables that map risks, threats, and vulnerabilities with potential countermeasures and countermeasure considerations.
- Develop a risk mitigation plan outline for an IT infrastructure.
- Use style and vocabulary generally appropriate to the message and intended audience.

## Assignment Requirements

- **IT Risk Management Plan:** IT Risk Management Plan draft aligned with the IT Risk Management Plan template. The IT Risk Management Plan is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Resources and citations are formatted according to APA (6th edition) style and formatting.
- **Font and font size:** Times New Roman, 12 point.

### Course Resources

IT Risk Management Plan Template [DOCX]

## u08s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Internet to study:

- RSA Conference. (2012). [Webcast: Security awareness — maybe it's not about the users \[Video\] | Transcript](#). Retrieved from <http://www.youtube.com/watch?v=nyrMW3YlgaI>

## u08s1 - Learning Components

- Analyze the role that policies and procedures play in selection of specific tools and controls.
- Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.
- Develop an IT risk mitigation plan.

## Unit 9 >> Sustaining Risk Assessments Activities and Risk Mitigation

### Introduction

#### This week you will:

- Study tools specific to the risk found in the IT infrastructures of health care organizations.
- Study security and awareness training and organizational structures in place to sustain risk mitigation.

Ongoing risk mitigation requires structures that will sustain the risk mitigation efforts. These structures include developing user security awareness and training, and the roles and responsibilities involved in documentation of compliance policies and training.

These resources can help you learn more about tools for mitigating risk in health care organizations, and types of risk response plans to sustain risk mitigation.

Use the textbook to read:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 12, "Mitigating Risk With a Business Impact Analysis," pages 314–338.
  - Chapter 13, "Mitigating Risk With a Business Continuity Plan," pages 342–367.

Use the Internet to study:

- Lisbon, S., & Rice, E. (2017). [Case study: Information security risk assessment for a small healthcare clinic using the security risk assessment tool provided by HealthIT.gov \[PDF\]](#). Retrieved from [http://www.micsymposium.org/mics\\_2017\\_proceedings/docs/MICS\\_2017\\_paper\\_7.pdf](http://www.micsymposium.org/mics_2017_proceedings/docs/MICS_2017_paper_7.pdf)

### Learning Activities

## u09d1 - Risk Assessment Tools for Health Care Organizations

Health care organization compliance with HIPAA is critical. Small health care organizations often struggle with ensuring this, however. There are a number of risk assessment tools for health care organizations. These tools are both proprietary and open source. IT security professionals in these organizations need to be familiar with the range of tools available, their effectiveness, and their cost.

## Discussion Question

Read the following case study: *Case Study: Information Security Risk Assessment for a Small Healthcare Clinic using the Security Risk Assessment Tool Provided by HealthIT.gov*.

Consider the following questions in your post:

- What positive benefits and positive uses of the security risk assessment tool (SRA) provided by HealthIT.gov did the authors find?
- What drawbacks of this tool did the authors discuss?

Research other health care security risk assessment tools. Select one and compare it to the SRA provided by HealthIT.gov. Between the two tools, which would you recommend for the organization in the case study? Justify your choice.

Your initial discussion post must be submitted by 11:59 PM Thursday.

#### References

Lisbon, S., & Rice, E. (2017). Case study: Information security risk assessment for a small healthcare clinic using the Security Risk Assessment tool provided by HealthIT.gov. Retrieved from [http://www.micsymposium.org/mics\\_2017\\_proceedings/docs/MICS\\_2017\\_paper\\_7.pdf](http://www.micsymposium.org/mics_2017_proceedings/docs/MICS_2017_paper_7.pdf)

## Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

#### Course Resources

Graduate Discussion Participation Scoring Guide

[Case Study: Information Security Risk Assessment for a Small Healthcare Clinic Using the Security Risk Assessment Tool Provided by HealthIT.gov](#)

#### u09d1 - Learning Components

- Evaluate internal risk with respect to technology and people related to a specific scenario.
- Use style and vocabulary generally appropriate to the message and intended audience.
- Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.
- Analyze the advantages and disadvantages of various risk assessment methodologies.

#### u09d2 - Validating Compliance

It is not sufficient merely to develop user security and awareness training or even to make it available to users. It is equally important, particularly in a regulated environment, to be able to demonstrate proof of what training has been provided and how the user performed during that training.

## Discussion Questions

In your post, select and refer to an organization with which you are familiar or can research in substantial detail regarding the tools that are used to mitigate risk in the organization's information security.

- What tools are available to document completion and scoring of required security awareness training?
- How would policy be used as a factor in making sure that security awareness training documentation is created and maintained?
- What roles and responsibilities make up an effective procedure for documentation of awareness training compliance?
- Should awareness training be standardized or role based? Provide support for your position.

Your initial discussion post must be submitted by 11:59 PM Thursday.

## Response Guidelines

Return to the discussion by the end of the week to read and review the posts of your peers. Does anyone else's topic coincide with or complement your own? Post a comment and add questions to further explore the experiences of your classmates. Also, in your response, comment on a topic described by a peer. Remember to give credit to external sources in your post.

Your responses must be submitted by 11:59 PM Sunday.

#### Course Resources

Graduate Discussion Participation Scoring Guide

#### u09d2 - Learning Components

- Evaluate internal risk with respect to technology and people related to a specific scenario.

- Analyze the role that policies and procedures play in selection of specific tools and controls.
- Use style and vocabulary generally appropriate to the message and intended audience.

## u09s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Internet to study:

- Whitmore, W. (2013). [Security compliance: Using online resources to meet the HIPAA training and awareness requirements \[Video\] | Transcript](http://www.youtube.com/watch?v=hu8eOpZuMf0). Retrieved from <http://www.youtube.com/watch?v=hu8eOpZuMf0>

Use the Capella Library to study:

- Shannon, M. (2016). [CISA: Compliance vs. substantive testing \[Video\]](#). Skillssoft Ireland.
- Skillssoft. (n.d.). [IT security for end users: IT security fundamentals \[Tutorial\]](#).
- Lacoste, R. (n.d.). [CompTIA Security+ SY0-501: Policies, plans, and procedures \[Tutorial\]](#). Skillssoft.
- Welton, T. (2015). [IT security for end users: End user role in IT security \[Video\]](#). Skillssoft Ireland.

## u09s1 - Learning Components

- Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.
- Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.
- Develop an IT risk mitigation plan.

## Unit 10 >> Holistic IT Risk Management

### Introduction

#### This week you will:

- Study various types of risk management response plans.
- Develop a computer incident response teams (CIRT) plan to mitigate risk in the event of a security breach.

Risk management response plan include mitigating risk using a business impact analysis, or a business continuity plan, or a disaster recovery plan, or a CIRT plan, or a combination of any or all of these types of risk mitigation response plans. Each of these different types of risk mitigation response plans has a purpose and approach that can be applied in various organization contexts depending upon the needs of the organization and the identification of risk, threats, and vulnerabilities through risk assessment. Having an appropriate mix of risk mitigation plans provides a holistic approach to IT risk management.

The following resource will help you learn more about risk management response plans.

Use the textbook to read:

- Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.
  - Chapter 14, "Mitigating Risk With a Disaster Recovery Plan," pages 371–396.
  - Chapter 15, "Mitigating Risk With a Computer Incident Response Team Plan," pages 400–428.

### Learning Activities

## u10a1 - LAB: Creating a CIRT Response Plan for an IT Infrastructure

### Overview

A computer incident response team (CIRT) determines if a breach has occurred and how it must be handled. The CIRT team functions according to pre-defined actions described in a CIRT plan. When a security breach happens, the CIRT team will identify, analyze, and contain the security breach, and finally remove the cause of the breach. The CIRT team aids in all aspects of recovering from the breach. Based on the circumstances surrounding the breach, the CIRT team will improve its CIRT plan based on lessons learned. In this lab, you will describe how a CIRT plan can mitigate risk, identify where CIRT monitoring and security operations occur throughout an IT infrastructure, identify countermeasures and security controls that can mitigate risk, and develop a CIRT response plan. You can use the assessment worksheet included with the lab as a study guide, but you will not submit it with your lab report.

### Instructions

1. Complete Lab 10 in the lab manual.

2. Complete the lab report and insert the information from the report into the Computer Incident Response Team (CIRT) Plan template.
3. Complete the remaining sections of the CIRT plan as noted in the template.
4. Upload your completed CIRT plan to the assignment for this unit.

## Assignment Criteria

Your assignment must meet these criteria. Please refer to the scoring guide for this assignment.

- Describe how a CIRT plan helps mitigate risks across the seven domains of an IT infrastructure.
- Identify where CIRT security operations and monitoring occur across an IT infrastructure.
- Identify security controls and countermeasures that will mitigate risk across the IT infrastructure and which will aid in a security incident response.
- Create a CIRT response plan for an IT infrastructure using the six-step incident response methodology.
- Use style and vocabulary generally appropriate to the message and intended audience.

## Assignment Requirements

- **Computer Incident Response Team (CIRT) Plan:** Computer Incident Response Team (CIRT) Plan aligned with the Computer Incident Response Team (CIRT) Plan template. The Computer Incident Response Team (CIRT) Plan is considered a professional document and should therefore follow the corresponding Academic and Professional Guidelines, including single-spaced paragraphs.
- **Written communication:** Written communication is free of errors that detract from the overall message.
- **APA formatting:** Resources and citations are formatted according to APA (6th edition) style and formatting.
- **Font and font size:** Times New Roman, 12 point.

### Course Resources

Computer Incident Response Team Plan Template [DOCX]

[Academic and Professional Document Guidelines \[PDF\]](#)

### u10d1 - Course Reflections

Share the aspects of this course that you found most useful and describe how those skills will enhance your professional goals.

## Response Guidelines

You are encouraged to share with your peers how their participation has helped your understanding of the topics covered in the course, but you are not required to post responses.

### Course Resources

Graduate Discussion Participation Scoring Guide

### u10d1 - Learning Components

- Use style and vocabulary generally appropriate to the message and intended audience.

### u10s1 - Topic Resources

Refer to these resources if you need clarification or additional support on the topics of this unit.

Use the Internet to study:

- RSA Conference. (2013). [Webcast: Mitigating the top human risks \[Video\]](#) | [Transcript](#). Retrieved from <http://www.youtube.com/watch?v=g7TNgBH6tQI>

Use the Capella Library to study:

- Skillsoft. (n.d.). [CISSP: Risk management \[Tutorial\]](#).

- Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.
- Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.
- Develop an IT risk mitigation plan.

**Scoring Guides**

**u01a1 - LAB: Identifying Threats and Vulnerabilities in an IT Infrastructure Scoring Guide**

Percentage of Course Grade: 5%.

Criteria	Non-performance	Basic	Proficient	Distinguished
Identify common risks, threats, and vulnerabilities that can be found in an IT infrastructure. 22%	Does not identify common risks, threats, and vulnerabilities that can be found in an IT infrastructure.	Identifies common risks, threats, and vulnerabilities that can be found in an IT infrastructure, although the identification is limited in scope.	Identifies common risks, threats, and vulnerabilities that can be found in an IT infrastructure.	Identifies common risks, threats, and vulnerabilities that can be found in an IT infrastructure and provides a rationale for the selection of risks, threats, and vulnerabilities.
Align the identified risks, threats, and vulnerabilities to each of the seven domains of a typical IT infrastructure. 23%	Does not align the identified risks, threats, and vulnerabilities to each of the seven domains of a typical IT infrastructure.	Aligns the identified risks, threats, and vulnerabilities to only some the domains of a typical IT infrastructure, or some of the alignments are not accurate.	Aligns the identified risks, threats, and vulnerabilities to each of the seven domains of a typical IT infrastructure.	Aligns the identified risks, threats, and vulnerabilities to each of the seven domains of a typical IT infrastructure and provides a rationale for the alignments.
Describe how identified risks can impact each of the seven domains of an IT infrastructure. 22%	Does not describe how identified risks can impact each of the seven domains of an IT infrastructure.	Describes how identified risks can impact only some of the domains of an IT infrastructure.	Describes how identified risks can impact each of the seven domains of an IT infrastructure.	Describes how identified risks can impact each of the seven domains of an IT infrastructure and provides specific examples.
Determine which of the domains of an IT infrastructure is most impacted by an identified risk, threat, or vulnerability. 23%	Does not determine which of the domains of an IT infrastructure is most impacted by an identified	Determines domains of an IT infrastructure impacted by an identified risk, threat, or vulnerability, but does not specify the	Determines which of the domains of an IT infrastructure is most impacted by an identified risk, threat, or vulnerability.	Determines which of the domains of an IT infrastructure is most impacted by an identified risk, threat, or vulnerability

	risk, threat, or vulnerability.	domain most impacted.		and provides specific examples of the impact.
Use style and vocabulary generally appropriate to the message and intended audience. 10%	Does not use style and vocabulary appropriate to the message and intended audience.	Uses style and vocabulary somewhat appropriate to the message and intended audience.	Uses style and vocabulary generally appropriate to the message and intended audience.	Uses style and vocabulary fully appropriate to the message and intended audience.

**u02a1 - Course Project: Draft IT Risk Management Plan Scoring Guide**

Percentage of Course Grade: 5%.

Criteria	Non-performance	Basic	Proficient	Distinguished
Write objectives for an IT risk management plan. 30%	Does not write objectives for an IT risk management plan.	Writes objectives for an IT risk management plan, but the objectives are poorly written or inaccurate for a given context.	Writes objectives for an IT risk management plan.	Writes objectives for an IT risk management plan that are comprehensive for a given context.
Write a scope statement for an IT risk management plan. 30%	Does not write a scope statement for an IT risk management plan.	Writes a scope for an IT risk management plan, but the scope is poorly written or inaccurate for a given context.	Writes a scope for an IT risk management plan.	Writes a scope for an IT risk management plan that is concisely written and comprehensive for a given context.
Write the roles and responsibilities for an IT risk management plan. 30%	Does not write the roles and responsibilities for an IT risk management plan.	Writes the roles and responsibilities for an IT risk management plan, but the roles are poorly described or incomplete for a given context.	Writes the roles and responsibilities for an IT risk management plan.	Writes the roles and responsibilities for an IT risk management plan that are concisely written and comprehensive for a given context.
Use style and vocabulary generally appropriate to the message and intended audience. 10%	Does not use style and vocabulary appropriate to the message and intended audience.	Uses style and vocabulary somewhat appropriate to the message and intended audience.	Uses style and vocabulary generally appropriate to the message and intended audience.	Uses style and vocabulary fully appropriate to the message and intended audience.

**u03a1 - LAB: Defining the Scope and Structure for an IT Risk Management Plan Scoring Guide**

Percentage of Course Grade: 10%.

--	--	--	--	--

Criteria	Non-performance	Basic	Proficient	Distinguished
Describe the process for IT risk management. 22%	Does not describe the process for IT risk management.	Describes the process for IT risk management, but the description is vague or missing key steps.	Describes the process for IT risk management.	Describes the process for IT risk management and provides an in-depth description of the activities that occur within the process steps.
List the risks, threats, and vulnerabilities for each domain of an IT infrastructure. 23%	Does not list the risks, threats, and vulnerabilities for each domain of an IT infrastructure.	Lists the risks, threats, and vulnerabilities for only some of the domains of an IT infrastructure, or the list has inaccuracies.	Lists the risks, threats, and vulnerabilities for each domain of an IT infrastructure.	Lists the risks, threats, and vulnerabilities for each domain of an IT infrastructure and provides a rationale for the selection of risks, threats, and vulnerabilities.
Describe the impact risk has for each identified threat. 22%	Does not describe the impact risk has for each identified threat.	Describes the impact risk has for only some of the identified threats.	Describes the impact risk has for each identified threat.	Describes the impact risk has for each identified threat and provides specific examples.
Relate identified risks, threats, and vulnerabilities and the potential impact of each in an IT risk management plan for a given organizational context. 23%	Does not relate identified risks, threats, and vulnerabilities and the potential impact of each in an IT risk management plan for a given organizational context.	Relates some of the identified risks, or some of the threats, or some of the vulnerabilities and the potential impacts in an IT risk management plan for a given organizational context.	Relates identified risks, threats, and vulnerabilities and the potential impact of each in an IT risk management plan for a given organizational context.	Relates identified risks, threats, and vulnerabilities and the potential impact of each in an IT risk management plan for a given organizational context and provides specific examples.
Use style and vocabulary generally appropriate to the message and intended audience. 10%	Does not use style and vocabulary appropriate to the message and intended audience.	Uses style and vocabulary somewhat appropriate to the message and	Uses style and vocabulary generally appropriate to the message and	Uses style and vocabulary fully appropriate to the message and intended audience.

## u04a1 - LAB: Performing a Qualitative Risk Assessment for an IT Infrastructure Scoring Guide

Percentage of Course Grade: 10%.

Criteria	Non-performance	Basic	Proficient	Distinguished
Define the purpose and objectives of an IT risk assessment. 18%	Does not define the purpose and objectives of an IT risk assessment.	Defines the purpose and objectives of an IT risk assessment, but the definition is vague.	Defines the purpose and objectives of an IT risk assessment.	Defines the purpose and objectives of an IT risk assessment that are comprehensive for a given context.
Align the identified vulnerabilities, threats, and risks to an IT risk assessment that incorporates the seven domains of a typical IT infrastructure. 17%	Does not align the identified vulnerabilities, threats, and risks to an IT risk assessment that incorporates the seven domains of a typical IT infrastructure.	Aligns the identified vulnerabilities, threats, and risks to an IT risk assessment that incorporates only some of the domains of a typical IT infrastructure, or some of the alignments are inaccurate.	Aligns the identified vulnerabilities, threats, and risks to an IT risk assessment that incorporates the seven domains of a typical IT infrastructure.	Aligns the identified vulnerabilities, threats, and risks to an IT risk assessment that incorporates the seven domains of a typical IT infrastructure and provides a rationale for the alignments.
Classify identified vulnerabilities, threats, and risks based on a qualitative risk assessment template. 18%	Does not classify identified vulnerabilities, threats, and risks based on a qualitative risk assessment template.	Classifies some of the identified vulnerabilities, threats, and risks based on a qualitative risk assessment template.	Classifies identified vulnerabilities, threats, and risks based on a qualitative risk assessment template.	Classifies identified vulnerabilities, threats, and risks based on a qualitative risk assessment template and provides a rationale for the classification.
Prioritize classified vulnerabilities, threats, and risks based on the defined qualitative risk assessment scale. 17%	Does not prioritize classified vulnerabilities, threats, and risks based on the defined qualitative risk assessment scale.	Prioritizes some of the classified vulnerabilities, threats, and risks based on the defined qualitative risk assessment scale.	Prioritizes classified vulnerabilities, threats, and risks based on the defined qualitative risk assessment scale.	Prioritizes classified vulnerabilities, threats, and risks based on the defined qualitative risk assessment scale and provides a rationale for the prioritization.
Write an executive summary that addresses the risk assessment results and risk assessment impact, and provide recommendations to mitigate areas of noncompliance. 20%	Does not write an executive summary that addresses the risk assessment results and risk assessment impact, or provide recommendations to mitigate areas	Writes an executive summary that addresses either the risk assessment results or the risk assessment impact, or provides	Writes an executive summary that addresses the risk assessment results and risk assessment impact, and provides recommendations	Writes an executive summary that addresses the risk assessment results and risk assessment impact, and provides recommendations

	of noncompliance.	recommendations to mitigate areas of noncompliance, but is missing key elements.	to mitigate areas of noncompliance.	to mitigate areas of noncompliance specific to a given context.
Use style and vocabulary generally appropriate to the message and intended audience. 10%	Does not use style and vocabulary appropriate to the message and intended audience.	Uses style and vocabulary somewhat appropriate to the message and intended audience.	Uses style and vocabulary generally appropriate to the message and intended audience.	Uses style and vocabulary fully appropriate to the message and intended audience.

**u06a1 - LAB: Identifying Risks, Threats, and Vulnerabilities in an IT Infrastructure Using Nmap and Nessus Reports Scoring Guide**

Percentage of Course Grade: 5%.

Criteria	Non-performance	Basic	Proficient	Distinguished
Review an Nmap network discover and port scanning report and a Nessus software vulnerability report. 17%	Does not review an Nmap network discover and port scanning report and a Nessus software vulnerability report.	Reviews an Nmap network discover and port scanning report and a Nessus software vulnerability report, but the review is vague or missing key points.	Reviews an Nmap network discover and port scanning report and a Nessus software vulnerability report.	Reviews an Nmap network discover and port scanning report and a Nessus software vulnerability report and provides an in-depth description of the report details.
Identify minor, major, and critical software vulnerabilities from the Nessus vulnerability assessment scan report. 18%	Does not identify minor, major, and critical software vulnerabilities from the Nessus vulnerability assessment scan report.	Identifies some of the minor, major, and critical software vulnerabilities from the Nessus vulnerability assessment scan report.	Identifies minor, major, and critical software vulnerabilities from the Nessus vulnerability assessment scan report.	Identifies minor, major, and critical software vulnerabilities from the Nessus vulnerability assessment scan report and provides a rationale for why there are vulnerabilities.
Identify operating systems, applications, services, hosts, and open ports on devices from the Nmap scan report. 19%	Does not identify operating systems, applications, services, hosts, and open ports on devices from the Nmap scan report.	Identifies some of the operating systems, applications, services, hosts, and open ports on devices from the Nmap scan report.	Identifies operating systems, applications, services, hosts, and open ports on devices from the Nmap scan report.	Identifies operating systems, applications, services, hosts, and open ports on devices from the Nmap scan report and provides the significance of these

				network components to network security.
Use the Common Vulnerabilities and Exposures (CVE) online listing of software vulnerabilities and conduct searches on this site and describe the search results. 18%	Does not use the Common Vulnerabilities and Exposures (CVE) online listing of software vulnerabilities to conduct searches on this site.	Uses the Common Vulnerabilities and Exposures (CVE) online listing of software vulnerabilities to conduct searches on this site, but does not describe the search results.	Uses the Common Vulnerabilities and Exposures (CVE) online listing of software vulnerabilities to conduct searches on this site and describes the search results.	Uses the Common Vulnerabilities and Exposures (CVE) online listing of software vulnerabilities and conduct searches on this site and provides details and insight about the search results.
Download, install, and use Nmap to run a variety of vulnerability scans. 18%	Does not download, install, and use Nmap to run a variety of vulnerability scans.	Downloads, installs, and uses Nmap to run a variety of vulnerability scans, but does not describe the results of the vulnerability scans.	Downloads, installs, and uses Nmap to run a variety of vulnerability scans.	Downloads, installs, and uses Nmap to run a variety of vulnerability scans and provides details and insight about the vulnerability scans.
Use style and vocabulary generally appropriate to the message and intended audience. 10%	Does not use style and vocabulary appropriate to the message and intended audience.	Uses style and vocabulary somewhat appropriate to the message and intended audience.	Uses style and vocabulary generally appropriate to the message and intended audience.	Uses style and vocabulary fully appropriate to the message and intended audience.

**u07a1 - LAB: Developing a Risk Mitigation Plan Outline for an IT Infrastructure Scoring Guide**

Percentage of Course Grade: 10%.

Criteria	Non-performance	Basic	Proficient	Distinguished
Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure. 18%	Does not identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.	Identifies the scope for an IT risk-mitigation plan, but does not focus on the seven domains of a typical IT infrastructure.	Identifies the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.	Identifies the scope for an IT risk-mitigation plan that is comprehensive for a given context, focusing on the seven domains of a typical IT infrastructure.
Align the major parts of an IT risk mitigation plan in each of the seven domains of a typical IT infrastructure.	Does not align the	Aligns the major parts of	Aligns the major parts of	Aligns the major parts of an IT

18%	major parts of an IT risk mitigation plan in each of the seven domains of a typical IT infrastructure.	an IT risk mitigation plan to some of the domains of a typical IT infrastructure.	an IT risk mitigation plan in each of the seven domains of a typical IT infrastructure.	risk mitigation plan in each of the seven domains of a typical IT infrastructure and provides a rationale for the alignments.
Define the tactical risk-mitigation steps required to remediate the identified vulnerabilities, threats, and risks typically found in the seven domains of an IT infrastructure. 18%	Does not define the tactical risk-mitigation steps required to remediate the identified vulnerabilities, threats, and risks typically found in the seven domains of an IT infrastructure.	Defines the tactical risk-mitigation steps required to remediate some of the identified vulnerabilities, threats, and risks typically found in the seven domains of an IT infrastructure.	Defines the tactical risk-mitigation steps required to remediate the identified vulnerabilities, threats, and risks typically found in the seven domains of an IT infrastructure.	Defines the tactical risk-mitigation steps required to remediate the identified vulnerabilities, threats, and risks comprehensively for a given context typically found in the seven domains of an IT infrastructure.
Define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure. 18%	Does not define processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.	Defines processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure, but the definition is vague or missing key steps.	Defines processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure.	Defines processes and procedures required to maintain a security baseline definition for ongoing risk mitigation within the seven domains of an IT infrastructure that is specific to a given context.
Create an outline for an IT risk mitigation plan incorporating the seven domains of an IT infrastructure. 18%	Does not create an outline for an IT risk mitigation plan incorporating the seven domains of an IT infrastructure.	Creates an outline for an IT risk mitigation plan, but does not incorporate all of the seven domains of an IT infrastructure.	Creates an outline for an IT risk mitigation plan incorporating the seven domains of an IT infrastructure.	Creates an outline for an IT risk mitigation plan incorporating the seven domains of an IT infrastructure specific to a given context.
Use style and vocabulary generally appropriate to the message and intended audience. 10%	Does not use style and vocabulary appropriate to the message	Uses style and vocabulary somewhat appropriate to	Uses style and vocabulary generally appropriate to	Uses style and vocabulary fully appropriate to the message

and intended audience.

the message and intended audience.

the message and intended audience.

and intended audience.

u08a1 - Course Project: Final IT Risk Management Plan Scoring Guide

Percentage of Course Grade: 20%.

Criteria	Non-performance	Basic	Proficient	Distinguished
Write objectives for an IT risk management plan. 18%	Does not write objectives for an IT risk management plan.	Writes objectives for an IT risk management plan, but the objectives are poorly written or inaccurate.	Writes objectives for an IT risk management plan.	Write objectives for an IT risk management plan that are comprehensive for a given context.
Write a scope statement for an IT risk management plan. 18%	Does not write a scope statement for an IT risk management plan,	Writes a scope for an IT risk management plan, but the scope is poorly written or inaccurate.	Writes a scope statement for an IT risk management plan.	Writes a scope for an IT risk management plan that is concisely written and comprehensive for a given context.
Write the roles and responsibilities for an IT risk management plan. 18%	Does not write the roles and responsibilities for an IT risk management plan.	Writes the roles and responsibilities for an IT risk management plan, but the roles are poorly described or incomplete.	Writes the roles and responsibilities for an IT risk management plan.	Write the roles and responsibilities for an IT risk management plan that are concisely written and comprehensive for a given context.
Develop tables that map risks, threats, and vulnerabilities with potential countermeasures and countermeasure considerations. 18%	Does not develop tables that map risks, threats, and vulnerabilities with potential countermeasures and countermeasure considerations.	Develops tables that map some of the risks, threats, and vulnerabilities with potential countermeasures and countermeasure considerations.	Develops tables that map risks, threats, and vulnerabilities with potential countermeasures and countermeasure considerations.	Develops tables that map risks, threats, and vulnerabilities with potential countermeasures and countermeasure considerations specific to a given context.
Develop a risk mitigation plan outline for an IT infrastructure. 18%	Does not develop a risk mitigation plan outline for an IT infrastructure.	Develops a risk mitigation plan outline for an IT infrastructure, but the outline is missing key elements.	Develops a risk mitigation plan outline for an IT infrastructure.	Develops a risk mitigation plan outline for an IT infrastructure with specific details for a given context.
Use style and vocabulary generally appropriate to the message and intended audience. 10%	Does not use style and vocabulary appropriate to the message and intended audience.	Uses style and vocabulary somewhat appropriate to the message and intended audience.	Uses style and vocabulary generally appropriate to the message and intended audience.	Uses style and vocabulary fully appropriate to the message and intended audience.

Percentage of Course Grade: 15%.

Criteria	Non-performance	Basic	Proficient	Distinguished
<p>Describe how a CIRT plan helps mitigate risks across the seven domains of an IT infrastructure. 22%</p>	<p>Does not describe how a CIRT plan helps mitigate risks across the seven domains of an IT infrastructure.</p>	<p>Describes how a CIRT plan helps mitigate risks across some of the domains of an IT infrastructure.</p>	<p>Describes how a CIRT plan helps mitigate risks across the seven domains of an IT infrastructure.</p>	<p>Describes how a CIRT plan helps mitigate risks across the seven domains of an IT infrastructure and provides supporting examples.</p>
<p>Identify where CIRT security operations and monitoring occur across an IT infrastructure 22%</p>	<p>Does not identify where CIRT security operations and monitoring occur across an IT infrastructure.</p>	<p>Identifies some of the areas where CIRT security operations and monitoring occur across an IT infrastructure.</p>	<p>Identifies where CIRT security operations and monitoring occur across an IT infrastructure.</p>	<p>Identifies where CIRT security operations and monitoring occur across an IT infrastructure and provides supporting examples.</p>
<p>Identify security controls and countermeasures that will mitigate risk across the IT infrastructure and which will aid in a security incident response. 22%</p>	<p>Does not identify security controls and countermeasures that will mitigate risk across the IT infrastructure and which will aid in a security incident response.</p>	<p>Identifies some of the security controls and countermeasures that will mitigate risk across the IT infrastructure and which will aid in a security incident response.</p>	<p>Identifies security controls and countermeasures that will mitigate risk across the IT infrastructure and which will aid in a security incident response.</p>	<p>Identifies security controls and countermeasures that will mitigate risk across the IT infrastructure and which will aid in a security incident response. Provides a rationale for the selection of the security controls and countermeasures.</p>
<p>Create a CIRT response plan for an IT infrastructure using the six-step incident response methodology. 24%</p>	<p>Does not create a CIRT response plan for an IT infrastructure using the six-step incident response methodology.</p>	<p>Creates a CIRT response plan for an IT infrastructure, but does not use the six-step incident response methodology.</p>	<p>Creates a CIRT response plan for an IT infrastructure using the six-step incident response methodology.</p>	<p>Creates a CIRT response plan for an IT infrastructure using the six-step incident response methodology applied to a given context.</p>
<p>Use style and vocabulary generally appropriate to the message and intended audience. 10%</p>	<p>Does not use style and vocabulary appropriate to the message and intended audience.</p>	<p>Uses style and vocabulary somewhat appropriate to the message and intended audience.</p>	<p>Uses style and vocabulary generally appropriate to the message and intended audience.</p>	<p>Uses style and vocabulary fully appropriate to the message and intended audience.</p>