Preview: IT4076 : Security Management and Policies

Syllabus

Course Overview

This course covers hands-on security management practices through the study of security policies and procedures, risk management, and business continuity planning. Topics include: security and business need trade-offs, risk assessments, designing security policies and procedures and a business continuity plan, and enforcement of security policies and procedures.

Course Competencies

(Read Only)

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

1. Quantify risk.
2. Assess risk for an organization.
3. Create an appropriate security policy for an organization.
4. Develop a security emergency plan.
5. Communicate effectively.

Course Prerequisites

Prerequisite(s): IT3355, IT4803.

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.

Miscellaneous Item

Fundamentals of Data Protection and Disaster Recovery.

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.

- Anonymous. (2010). WikiLeaks "hactivists" target fax machines. *Informationweek–online*.
- Bayuk, J. L., Healey, J., & Rohmeyer, P. (2012). *Cyber security policy guidebook.* Hoboken, NJ: John Wiley & Sons.
- Engemann, K. J., & Henderson, D. M. (2012). *Business continuity and risk management: Essentials of organizational resilience.* Brookfield, CT: Rothstein Associates, Inc.

- LaRose, G. (2010, October 6). Rage against the fax machines. *New Orleans City Business.*
- McCrie, R. D. (2007). *Security operations management.* Burlington, MA: Butterworth–Heinemann.
- Moskowitz, J. (2010). *Group policy: Fundamentals, security, and the managed desktop.* Indianapolis, IN: Sybex.
- Potter, B. (2011, May/June). Coming to grips with security. *IT Professional, 13*(3), 14–17.
- Smallwood, R. F., & Blair, B. T. (2012). *Safeguarding critical e-documents: Implementing a program for securing confidential information assets.* Hoboken, NJ: John Wiley & Sons.
- Stewart, J. M., Chapple, M., & Gibson, D. (2012). *CISSP: Certified information systems security professional study guide* (6th ed.). Hoboken, NJ: John Wiley & Sons.
- Tammineedi, R. L. (2010, January). Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective, 19*(1), 36–50.
- Thomson, K. L., von Solms, R., & Louw, L. (2006, November 14). Cultivating an organizational information security culture. *Computer Fraud & Security,* 10, 7–11.

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.

- National Institute of Standards and Technology. (2010). *Guide for assessing the security controls in federal information systems and organizations: Building effective security assessment plans* (NIST Special Publication 800-53A). Gaithersburg, MD: Author. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf
- Saleh, Z. I., Refai, H., & Mashhour, A. (2011). Proposed framework for security risk assessment. *Journal of Information Security*. Retrieved from http://www.scirp.org/journal/PaperInformation.aspx?paperID=4724
- Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). Risk management guide for information technology systems (NIST Special Publication 800-30). *National Institute of Standards and Technology*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R. (2002, June). Contingency planning guide for information technology systems (NIST Special Publication 800-34). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
- U.S. Department of Health and Human Services: Centers for Medicare and Medicaid Services. (2010). CMS system security plan (SSP) procedure. Retrieved from http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/SSP_Procedure.pdf

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.

Projects

Project >> Policy, Risk and Business Continuity Plan

Project Overview

Your final project will include a revised and complete risk assessment and recommendations, a business continuity plan and a set of policy recommendations for the sample organization provided.

Scenario

Mark Moneybags has decided to use the millions of dollars he inherited from his rich uncle Mike to venture into the healthcare industry. To that end he has begun construction on a brand new 150-bed hospital called High Class Healthcare in a North Hennepin suburb. Construction is nearly complete, so Mark has begun to turn his attention to activities related to opening the hospital itself.

Recently Mark hired his executive tier, which is described in the organization chart for High Class Healthcare. They in turn have hired their immediate subordinates. It is this group of individuals upon whom Mark will rely to get his hospital up and running.

Tess Tekky, the newly appointed CIO for High Class Healthcare, has hired you to conduct a risk assessment and to develop recommendations for a business continuity plan and information security policies that High Class Healthcare can implement as part of opening for business.

Technical Details

Mark Moneybags, in coordination with Tess Tekky and Nick Network, has purchased a number of information assets that will be used to create, transmit and store the health data collected at High Class Healthcare. The specific items which have been purchased are listed on the Risk Assessment Template document. You should assume that the list is a complete set of information assets and that anything you believe missing from this list has not been purchased and should therefore be added to your risk recommendations.

The network for High Class Healthcare is being implemented exclusively using fiber and Cat5e cable. Mark Moneybags has opted to reserve implementation of a wireless network as a future enhancement to the network.

Fiber will be used only on the backbone between the core switches and to the segment where the ERP, EMR, and Radiology servers will be located. All other segments of the network will be implemented using Cat5e. Network speeds are 100 mg to the desktop and gigabit Ethernet on the backbone and server segments.

A computing facility has been constructed in the basement of the new building below the main kitchen. Proper racks and housing for the blade servers have been installed as part of the facility construction. Access to this area is controlled by short-range RFID badges that generate audit reports, which include both authorized and unauthorized access attempts. The dock and storage areas are located behind the computing facility, which requires staff for all of those areas to be given access. In addition, Ben Buildings, who is responsible for Facilities Management, has asked for access for himself and all of his staff who are responsible for security and environmental controls for the facility. Mark has agreed that this access is necessary in the event of an incident that would require this staff to have access to this area.

All servers will be located in the computing facility with the exception of the lab servers. Larry Labguy has had a bad experience with IT in the past, so he made it a condition of his employment that his servers will be housed in the second floor lab area and he will have administrator access to manage these servers himself. Larry has agreed to go out and purchase a UPS for the server, but there are no environmental or security controls designed for the lab area.

Mr. Moneybags and Nick have asked you to include recommendations for who should have access to which of these resources once the network is implemented. Currently Nick has provided domain administrator accounts to all of the executive leadership, including Larry Labguy. They in turn have also created domain administrator accounts for all of their immediate subordinates.

The network architecture being designed includes the use of Openlink as an interface engine, which will feed data streams between systems. All of the source systems will be those that send data and the receiving systems will be those who have data fields populated. The interfaces being developed are included in the risk assessment template.

Irene Invoice has pointed out the need to transmit large amounts of patient billing information to the clearinghouse with whom Mark has contracted for the purposes of communicating with the payers. She has suggested that these files be sent via FTP. Betsy BuysStuff would like a direct connection between High Class Health and their top 20 suppliers that would allow the suppliers to manage their own inventory items. Mark has asked for your opinion as part of your risk assessment recommendations.

Resource

- High Class Healthcare Organizational Chart.
- **Written communication:** Written communication should be free of errors that detract from the overall message.
- **Parts of a paper:**
  - A cover sheet.
  - An executive summary.
  - Final Risk Assessment Recommendations and Business Continuity Plan.
  - Related documents.

    - Properly formatted references.

- **Length of paper:** No page length requirements.
- **List of references:** A list of references, including books, Web sites, articles, and other resources.
- **Diagrams:** All diagrams must be done in an application such as Visio.
- **APA formatting:** Resources and citations should be formatted according to Capella's APA Style and Formatting guidelines.
- **Font:** Use Arial, 10-point.

Unit 1 >> Evaluation and Risk Assessment

Introduction

Whether it is better to write security policy first and then do a risk assessment, or to begin with the risk assessment and then write policy, is a bit of a chicken-and-egg conversation. In this course, you will be asked to work both ends at the same time.

You have been given the details of an organization that will be the basis for the assignments and course project. This week you will be asked to begin a risk assessment of this organization and come up with a sense of the threats and vulnerabilities that can potentially impact the information assets of your project organization.

You will also be asked to evaluate some policy resources in preparation for development of your own set of policy recommendations. The author of the text has come up with his list of appropriate Tier2 policies which you will also be evaluating in terms of how each specific policy fits or does not fit with your own set of recommendations in the final project.

You will learn about some of the legal implications of handling protected data as well as some of the laws that may have policy implications for which policies and practices are legally mandated.

Learning Activities

u01s1 - Studies

Readings

The reading material comes from the National Institute of Standards in Technology (NIST) special publications relating to risk management and mitigation. These materials will inform the Unit 1 assignment and discussion that involve potential sources of risk and risk assessment strategies.

In Risk Management Guide for Information Technology Systems (NIST SP800-30), read the following. (This publication will be referred to as NIST SP800-30 for the remainder of the course.)

- Sections 1, 2, 3, and 4, pages 1–38. Refer to the appendix items as you deem appropriate to fill in knowledge gaps.

In the Guide for Assessing the Security Controls in Federal Infromation Systems and Organizations (NIST SP800-53A), read the following. (This publication will be referred to as NIST SP800-53A for the remainder of the course.)

- Chapters 1, 2, and 3, pages 1–24. Refer to the appendix items as you deem appropriate to fill in knowledge gaps.

Self-Paced Tutorial

Capella University offers free interactive tutorials as part of this course. These tutorials offer guided practice in performing tasks related to course competencies. Complete the following:

- Go to the CISM 2012: Information Risk Management and Compliance (Part 1) tutorial.
    - Under the **Information Risk Assessment** lesson, complete the following topics:
        - Risk Identification.
        - Risk Analysis.

Technical Support

Capella provides Academic Technical Support to help learners with technical issues in courses. Visit the Online Technical Support Center if you have any issues with the Skillsoft self-paced tutorials.

Skillsoft Tutorial Maintenance Windows

Please note: Skillsoft self-paced tutorials will be unavailable due to maintenance during the following times each week:

- Wednesdays 12:00 AM and 1:00 AM CST.
- Sundays 12:00 PM and 2:00 PM CST.

Accessible Versions Available

If you require the use of assistive technology such as a screen reader to use these tutorials, please contact Academic Technical Services for accessible versions of these tutorials.

Course Resources

National Institute of Standards and Technology. (2010). *Guide for assessing the security controls in federal information systems and organizations: Building effective security assessment plans* (NIST Special Publication 800-53A). Gaithersburg, MD: Author. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

u01s2 - Project - Preparation

Read the Policy, Risk and Business Continuity Plan course project description to learn the requirements for your course project.

u01v1 - Optional Unit 1 Virtual Lab 1

u01a1 - Risk Assessment

Use the resources provided and the project description to determine areas of potential vulnerability within the organization and to complete an organizational IT risk assessment for this organization. An Excel spreadsheet is provided for documenting the results of your risk assessment.

When complete, submit your document in the assignment area.

Course Resources
Risk Assessment Documentation spreadsheet
Risk Management Guide for Information Technology Systems

u01d1 - Common Threats and Vulnerabilities

Read the Discussion Participation Scoring Guide to learn how the instructor will evaluate your discussion participation throughout this course.

You have been asked to present a paper at a local conference on current threats and vulnerabilities facing information security professionals around the world. In preparation for this presentation, discuss your perspective as to what you would highlight as concerns at the forefront in the security community. Include in the discussion your experience with any of these threats (impact) and how widespread (likelihood) you believe they might be. Also discuss what resources may be available on the Internet to help identify new and persisting threats.

Response Guidelines

Respond to at least one other learner who has identified different threats and vulnerabilities than your own, and tell them whether you agree or disagree with their findings.

Course Resources
Undergraduate Discussion Participation Scoring Guide

u01s3 - Software Preparation and Technology Access

In this course, you will be using software and technology that is needed to complete designated activities and assignments. There is no additional cost for this software and technology. Some software packages will be made available to you at no additional cost through Capella's subscription with Microsoft, while other software packages are available for free download through open-source licensing.

Capella University requires learners to meet certain minimum computer requirements. Please note that some software required for a course may exceed these minimum requirements. Check the requirements for the software you may need to download and install to make sure it will work on your device. Most software will require a Windows PC. If you use a Mac, refer to Installing a Virtual Environment and Windows on a Mac.

The software and technologies below are strongly recommended to support you in completing the course objectives. If you have access to other tools that you believe may still meet the requirements of this course, please discuss your selected alternatives with your instructor.

If you use assistive technology or any alternative communication methods to access course content, please contact Disability Services with any access-related questions or to request accommodations.

For this course, follow the instructions provided through the links below to download and install software or register for an account, as required.

Microsoft Software

1. If you have a Capella MS Imagine account, go to Step 2. Otherwise, see the instructions for registering an account at MS Imagine – Registration.
2. Log into the Capella Microsoft Imagine WebStore.
3. Identify the version of MS Visio that is compatible with your operating system.
4. Download and install.

Unit 2 >> Reporting and Recommendations

Introduction

Last week you were asked to identify the threats and vulnerabilities that may impact the information security assets of your project organization. This week you will be asked to identify controls that can be used to manage

those threats and vulnerabilities. These controls may be in the form of hardware, software, procedures, policies or any other combination of these that best address the circumstances.

Unless you have had occasion to look for specific controls it is likely that you do not know how to go about that. The expectation is not that you recommend a Cisco PIX but rather that you recommend a firewall. While information security is still an immature industry, there are core practices that should simplify the selection of commonly used solutions to mitigate specific threats.

You will have another opportunity to evaluate sample policies for content and fit with your policy development project.

Finally, you will be asked to consider the role that project management methodologies play in support of a policy development project, and you will be given some tools to use that will help keep your project on track.

Learning Activities

u02s1 - Studies

This unit's readings cover the creation of an information security risk frameworks and models as tools to support the work of risk assessment and policy development. The risk material will inform the Unit 2 assignment involving the completion of the risk assessment that began in Unit 1. The Unit 2 discussion is related to the role of standards in the creation of information security policy.

Readings

Use the Internet to complete the following:

- Saleh, Refai, and Mashhour's 2011 article, "Proposed Framework for Security Risk Assessment" from the *Journal of Information Safety*, volume 2, issue, 2 page 85.
- Potter's 2011 article, "Coming to Grips with Security" from IT Professional, volume 13, issue 3, pages 14–17.
- Thomson, von Solms, and Louw's 2006 article, "Cultivating an Organizational Information Security Culture" from *Computer Fraud & Security,* issue 10, pages 7–11.

Self-Paced Tutorials

Complete the following:

- Go to the CompTIA Advanced Security Practitioner (CASP) (Exam CAS-001): Managing Risk, Security Policies, and Security Procedures (Part 6 of 8) tutorial:
  - Under the **Analyze Security Risk** lesson, complete all of the topics.
- Go to the CISM 2012: Information Risk Management and Compliance (Part 1) tutorial.
  - Under the **Information Risk Assessment** lesson, complete the following topics:

- Risk Assessment Methodologies.
- Practicing Risk Assessment.

u02a1 - CIO Report

Write a formal risk assessment summary report to the CIO of the project based on the data you gathered during last week's risk assessment.

Be sure to include the following:

- A brief introduction to set the stage for what is included in the report.
- A description of the factors specific to the particular organization that impact risk.
- Identification of areas of highest risk based on likelihood and impact and explanation of why they are of particular importance.
- Recommendation of controls that can be used to mitigate the particular risks that you have identified and support for why they are the optimal control to apply for this particular risk mitigation.
- A summary of the important points that make up the paper.
- APA references and citations.

If you choose to submit charts or spreadsheets from earlier work, do so as appendices to the document.

When complete, submit your documents in the assignment area.

Course Resources
Risk Assessment Documentation spreadsheet
Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans
Risk Management Guide for Information Technology Systems

u02d1 - The Role of Standards in Policy Development

You have been asked to give a presentation on the role that standards will play in the creation of an information security policy for your project organization. Discuss the existing standards that play a role in this process. Include in the discussion whether or not you would select a specific standards setting body for guidance in creating these policies and procedures. Also include in the discussion the relative advantages and disadvantages of implementing standards for the organization.

Response Guidelines

Respond to at least one other learner and share one additional advantage that comes with implementing standards that they did not include in their response.

Course Resources
Undergraduate Discussion Participation Scoring Guide

Unit 3 >> Creating Information Security Policies

Introduction

Now that you have established the threats and vulnerabilities that may impact the information assets of the organization and have developed a list of mitigating controls, it is time to evaluate the level of risk. You must do this before you determine which of these controls best balances risk and benefit.

Risk is based on two dimensions known as likelihood and impact. These two dimensions can be combined into a matrix and measured as high, medium and low. This creates 4 zones of risk, which are useful in prioritizing the work of mitigation. Those items that fall into the high impact and high likelihood zone are deserving of the most immediate attention, while those items that are low impact and low likelihood may not be worthy of mitigation at all.

You will have another opportunity to evaluate sample policies for content and fit with your policy development project.

You will also learn about the project management steps towards implementation of a policy development project and the role of the data owner, data custodian and data users that are impacted by the process.

Learning Activities

u03s1 - Studies

Internet and Library Research

Use the following keywords to research concepts related to creation of an information security policy planning, development, implementation team and associated resources which will support the Unit 3 assignment and discussion.

- Information security policy planning.
- Information security policy team.
- Information security policy roles and responsibilities.
- Computer security policy planning.
- Computer security policy team.
- Computer security policy roles and responsibilities.
- Computer security policy framework.
- Information security policy framework.
- Components of an enterprise computer security policy plan.
- Components of an enterprise information security policy plan.
- Components of a computer security policy implementation project.
- Components of an information security policy implementation project.
- Information security policy template.
- Computer security policy template.
- Computer security policy samples.
- Information security policy samples.
- Computer security policy examples.
- Information security policy examples.
- Assessing likelihood of information security risk.
- Assessing likelihood of computer security risk.
- Computer security risk assessment likelihood.
- Information security risk assessment likelihood.

u03a1 - Security Policy

Using the resources provided and the project description create a proposal that includes the following topics:

- Identify specific members of the project organization to form the policy creation team and provide support for your selection.
- Create a list of specific information security policies that will be created by this team (if this list differs from the 10 domains recommended in the required reading include support for why you are recommending an

alternate approach).
- Design a policy template that all team members will use to create uniform policies and provide support for your selection.

Course Resources
Risk Impact Matrix
Risk Assessment Documentation spreadsheet
Risk Management Guide for Information Technology Systems
Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans

u03d1 - Estimating Likelihood

In your role as a highly paid consultant you are given a list of potential threats and vulnerabilities to the information assets of an organization. You are asked to provide quantitative data to measure the likelihood that any of these threats will actually occur to the information assets of the client. Do some research and come back and share with the class what resources you found that might provide insight into measuring the likelihood that some of the threats would actually occur. Include in the discussion whether you see a trend in resources that might indicate a specific industry is particularly involved in gathering this kind of data.

Response Guidelines

Respond to at least one other learner and share with them why one of your particular resources is particularly helpful in measuring threat related data.

Course Resources
Undergraduate Discussion Participation Scoring Guide

Unit 4 >> Asset Clarification

Introduction

This week you will be asked to create a final list of specific controls that can be used to manage the threats and vulnerabilities to your project organization. These controls may be in the form of hardware, software, procedures, policies or any other combination of these that best address the specific concern while integrating properly with other control layers you are proposing.

All controls you recommend should be evaluated in the context of:

- Effectiveness.
- Regulatory requirements.
- Compatibility with the environment.
- Cost to include support costs.
- Safety.

You will have another opportunity to evaluate sample policies for content and fit with your policy development project.

Finally, you will be asked to create a final set of recommendations for submission to the CIO of your project organization.

Learning Activities

u04s1 - Studies

Your readings for this unit cover asset classification with a particular emphasis on data classification. The Unit 4 assignment and discussion topics are also focused on data classification.

Readings

Read the following chapters from Smallwood & Blair's 2012 book *Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets*.

- Chapter 1 "The Problem: Securing Confidential Electronic Documents," pages 3 – 12.
- Chapter 2, "Information Governance: The Crucial First Step," pages 13 – 26.
- Chapter 15, "Safeguarding Confidential Information Assets: Where do you Start?" pages 187 – 196.

Internet and Library Research

Use the following keywords to research concepts related to asset classification and the role it plays as part of an information security policy plan which will support completion of the unit assignment and discussion

- Information security asset classification.
- Computer security asset classification.
- Information security policy asset classification.
- Computer security policy asset classification.
- Information security asset classification roles and responsibilities.
- Computer security asset classification roles and responsibilities.
- Information security asset classification challenges and risks.
- Computer security asset classification challenges and risks.
- Information security asset classification benefits.
- Computer security asset classification benefits.

u04a1 - Data Classification Program

Using the resources provided and the project description to create a data classification project proposal that includes the following topics:

- An introduction to set the stage for what is included in the report.
- The roles and responsibilities involved with location and classification of the data.
- The risks and benefits of engaging in an asset classification program.
- Potential strategies for mitigating the risks of data classification.
- Potential strategies for maximizing the benefits of data classification.
- A summary of the important points that make up the paper.
- APA references and citations.

When complete, submit your document in the assignment area.

u04d1 - Security versus Availability

You join a group of information security professionals for lunch one day and a member of the group describes a project he is working on for a client that involves classification of the core data that runs the business processes of the organization. He is meeting resistance from the users who have become aware of new restrictions that will be placed on data relative to its classification.

Do you agree that data classification controls should be implemented as one of the security layers that manage access to data? If so, discuss what controls you would recommend and how you will avoid impeding the necessary work of the users who are not accustomed to restrictions on their access to organizational data.

If you do not agree that controls should be implemented, support your position.

Response Guidelines

Respond to at least one other learner and share a control they did not consider, including support for why it would be a useful addition to their plan. Or respond to at least one other learner who does not support the use of data classification controls and share why you agree or disagree with their position.

Course Resources

Undergraduate Discussion Participation Scoring Guide

Unit 5 >> Personnel Security Policy

Introduction

Contingency planning has taken on more importance for many organizations following widely publicized disasters such as Katrina and the 9/11 attacks. Development of new technology has been a huge benefit to organizations in improving operations, accuracy and speed. It presents a challenge in that information assets and data have become an organization's most important assets.

This week you will begin looking at some of the strategies that are used to ensure an organization is capable of continuing to operate following an emergency. You will begin by learning about contingency planning policy, and how it fits with the business continuity planning process.

You will have another opportunity to evaluate sample policies for content and fit with your policy development project.

Finally you will be asked to create a business continuity planning policy statement for your project organization.

Course Resources

Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R. (2002, June). Contingency planning guide for information technology systems (NIST Special Publication 800-34). Retrieved from

http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Learning Activities

u05s1 - Studies

The reading material covers concepts related to personnel security, which is also the focus of the Unit 5 assignment and discussion.

Readings

Read the following chapters from Bayuk, Healey, and Rohmeyer's 2012 book *Cyber Security Policy Guidebook*.

- Introduction, pages 1 – 14.
- Section 3.5, "Security Policy Objectives," pages 67 – 68.
- Section 4.2, "Policy as a Project," pages 71 – 73.
- Section 5.2, "Cyber Security Policy Taxonomy," pages 89 – 92.
- Section 6.2, "Cyber User Issues," pages 112 – 140.

Read the following chapter from Moskowitz's 2010 book *Group Policy: Fundamentals, Security, and the Managed Desktop*.

- Chapter 8 "Implementing Security with Group Policy," pages 437 – 552.

u05d1 - Personnel Security

As CIO of a local marketing firm you have been asked to offer your opinion on a proposed change within the Human Resources department. Currently employees are hired mostly by word of mouth as known associates of existing employees. This process has served the marketing firm well enough and there have been no incidents of bad hires as a result of this practice.

Now the head of the HR department has attended a seminar offered by the Department of Homeland Security which suggested that organizations conduct thorough background checks, including collection of fingerprints, prior to offering a position. Discuss your opinion as it relates to this suggestion. Include in the discussion any risks and benefits of implementing this practice. Also include in the discussion your perspective as to whether or not this violates the applicant's personal privacy.

Response Guidelines

Respond to at least one other learner and tell them why you agree or disagree with their position.

Course Resources

Undergraduate Discussion Participation Scoring Guide

u05a1 - Personnel Security Policy

Using the resources provided and the project description, complete the policy template that you created in Unit 3 to draft a personnel security policy appropriate for the project organization. Ensure that the following information is covered in the policy language proposed:

- Factors that are included within the scope of a personnel security policy.
- Roles and responsibilities that are involved with the various activities included in the policy.
- Application of contextual characteristics specific to the project organization.
- Policy noncompliance procedures and penalties.

When complete, submit your document in the assignment area.

Course Resources

Contingency Planning Guide for Information Technology Systems

Unit 6 >> Physical and Environmental Security Policy

Introduction

Most organizations rely on a variety of information assets to function day to day. Before experiencing a serious outage or major disaster, it is essential to evaluate and document all of these information assets. Once documented, it is important to assign priorities to these assets to prevent confusion and unnecessary delay in the event of a disaster.

This week you will be asked to create a Business Impact Analysis for your project organization. You will find this analysis to be similar to the threat and likelihood matrix that you completed in an earlier unit.

You will have another opportunity to evaluate sample policies for content and fit with your policy development project.

Finally you will be asked to discuss the role that standards play in the creation of policies and in the development of your Business Continuity Plan.

Learning Activities

u06s1 - Studies

Internet and Library Research

Use the following keywords to research concepts related to physical and environmental information security policy which will support completion of the unit assignment and discussion

- Information security environmental policy.
- Computer security environmental policy.
- Information security computing facility policy.
- Computer security computing facility policy.
- Computing facility environmental policy.
- Computing facility physical security policy.
- Wiring closet environmental policy.
- Wiring closet physical security policy.
- Information security physical security policy.
- Computer security physical security policy.
- Information technology physical security roles and responsibilities.
- Information technology environmental security roles and responsibilities.
- Information technology environmental security policy.
- Information technology physical security policy.
- Integration of physical and logical security.
- Responsibilities of a CSO (Computer Security Officer).
- Impact of physical security on information assets.
- Impact of environmental security on information assets.

u06a1 - Physical and Environmental Security Policy

Using the resources provided and the project description, complete the policy template that you created in Unit 3 to draft physical and environmental security policy or policies appropriate for the project organization. Ensure

that the following information is covered in the policy language proposed:

- Factors that are included within the scope of a physical and environmental security policy.
- Roles and responsibilities that are involved with the various activities included in the policy.
- Application of contextual characteristics specific to the project organization.
- Policy noncompliance procedures and penalties.

When complete, submit your document in the assignment area.

u06d1 - The Integration of Physical and Logical Security

You have been hired by a large software development organization to review and recommend to their senior managers whether or not to create a new executive spot that will combine physical and information security activities. Discuss what factors you would consider as part of making such a recommendation. Include in the discussion your position on the integration of physical and information security as a general concept as well as how it might apply to this particular situation.

Response Guidelines

Respond to at least one other learner and share with them how their posting helped to solidify your understanding of the concepts.

Course Resources
Undergraduate Discussion Participation Scoring Guide

Unit 7 >> Preventative Controls and Recovery Strategies

Introduction

This week you will be reviewing the creation of preventative controls and recovery strategies, which will be similar to the work you did in a previous unit. Using this additional information, you can go back to the controls you have recommended and re-evaluate them in light of the additional information.

Having a plan in place for an alternate site is an important component of a Business Continuity Plan. You will be asked to discuss the various alternatives that are available to someone engaged in this work and to explore the relative advantages and disadvantages of implementing each of them.

You will have another opportunity to evaluate sample policies for content and fit with your policy development project.

Finally you will be asked to create a set of procedures, using one of the suggested formats in the text, for backing up data for your project organization.

Learning Activities

u07s1 - Studies

The reading material covers various aspects of operational security, including a sample security plan and examples of communication device–related security concerns, which are the focus of the Unit 7 assignment.

Readings

Use your textbook, the Capella Library, and the Internet to complete the following:

- In McCrie's 2011 book, Security Operations Management,
  - Read Chapter 1, "Security Operations in the Management Environment," pages 3 – 28.
  - Read Chapter 10, "Operating Physical- and Technology-Centered Programs," pages 285–318.
- In Stewart, Chapple, and Gibson's 2012 book CISSP: Certified Information Systems Security Professional Study Guide,
  - Read Chapter 13, "Security Operations," pages 531 – 570.
- The U.S. Department of Health and Human Services Centers for Medicare and Medicaid Services' 2010 article, "CMS System Security Plan (SSP) Procedure."
- LaRose's 2010 article, "Rage against the Fax Machines," in *New Orleans City Business*.
- Anonymous' 2010 article, "WikiLeaks "Hactivists" Target Fax Machines," in *Informationweek–online*.

Internet and Library Research

Use the following keywords to research concepts related to selection of a disaster recovery alternate site which supports completion of the unit discussion.

- Disaster recovery hot site.
- Disaster recovery cold site.
- Disaster recovery warm site.
- Disaster recovery site co-location.
- Disaster recovery mobile site.

- Disaster recovery site selection examples.
- Disaster recovery site selection tutorials.
- Information technology disaster recovery plan.
- Information technology disaster recovery resources.

u07a1 - Operational Management Policies

Using the resources provided and the project description, complete the policy template that you created in Unit 3 to draft operational management policies appropriate to cover the functional areas related to operational management for the project organization.

Ensure that the following information is covered in the policy language proposed:

- Factors that are included within the scope and range of operational management security policies.
- Roles and responsibilities that are involved with the various activities included in the policies.
- Elements of a communication plan that will be used to support the creation of these operational management security policies.
- Application of contextual characteristics specific to the project organization.
- Policy noncompliance procedures and penalties.

When complete, submit your document in the assignment area.

u07d1 - Hot, Warm, and Cold Sites

You are a newly hired CIO of a large healthcare organization that has 3 hospitals and 17 clinics in 4 conjoined states. Due to the HIPAA requirements that organizations must engage in Business Continuity Planning, one of your first assignments is to evaluate potential disaster recovery sites that can be used in the event of a catastrophic event at one or more of the sites. Discuss the factors that you will include in your consideration for alternate sites. Also discuss the relative advantages and disadvantages of available options.

Response Guidelines

Respond to at least one other learner who had a solution different than yours and share which you prefer and why.

Course Resources

Undergraduate Discussion Participation Scoring Guide

Unit 8 >> Access Control and Software Development and Maintenance Policies

Introduction

Donn Parker, who is considered one of the grandfathers of the information security industry, believes that policies are always onerous and viewed by users as a barrier to their individuality and creativity. He is of the opinion that policies must be implemented in such a way so that understanding and compliance is periodically evaluated as a component of the employee's performance. Some organizations that are in regulated industries, such as healthcare, have begun to implement an annual online training as a means to document for HIPAA that employees are trained in healthcare information security and privacy. This week you will be asked to discuss strategies to ensure that policies are both understood and enforced.

There is a certain amount of controversy about the actual impact of a catastrophic event on a business. Some would say as many as 80 to 90 percent of businesses fail after such an event, and others believe that this figure is not well researched and is probably too high. Regardless, having an effective business contingency plan and ensuring that it is well tested and kept up to date is an important aspect of securing the information assets of the organization. This week you will finalize the business continuity plan for your project organization.

Learning Activities

u08s1 - Studies

Your readings for this unit cover access control policies and policies and procedures related to system maintenance and software development security, which are focus areas within the Unit 8 assignment and discussion.

Readings

Read the following chapters from Stewart, Chapple, and Gibson's 2012 book *CISSP: Certified Information Systems Security Professional Study Guide*.

- Chapter 1, "Access Control," pages 1–46

- Chapter 7, "Software Development Security," pages 275–326.

Internet and Library Research

- Information security access control policy.
- Computer security access control policy.
- Computer system user access policy.
- Data security access control policy.
- Software development security policy.
- Software maintenance security policy.
- Operating system maintenance security policy.
- Information security policy non-compliance.
- Computer security policy non-compliance.
- Data security policy non-compliance.
- Communicating information security policy.
- Disseminating information security policy.
- Communicating computer security policy.
- Disseminating computer security policy.
- Communicating data security policy.
- Disseminating data security policy.
- Communicating cyber security policy.
- Disseminating cyber security policy.

Self-Paced Tutorial

Complete the following:

- Go to the Fundamentals of Data Protection and Disaster Recovery tutorial:
  - Disaster Recovery: Concepts and Techniques.
  - Creating and Implementing Disaster Recovery Plans.

u08a1 - Access Control, Software Development, and Maintenance

Using the resources provided and the project description, complete the policy template that you created in Unit 3 to draft access control and software development and maintenance security policies appropriate to cover the functional areas related to operational management for the project organization.

Ensure that the following information is covered in the policy language proposed:

- Factors that are included within the scope and range of access control and software development and maintenance security policies.
- Roles and responsibilities that are involved with the various activities included in the policies.
- Application of contextual characteristics specific to the project organization.
- Policy noncompliance procedures and penalties.

When complete, submit your document in the assignment area.

u08d1 - Selling Policies

You have come close to completion of your policy development project for your project organization. Using the resources provided in the text as well as your own personal experience with policy implementation, discuss how you will sell these policies to the organization to ensure that they are both widely understood and adopted. Include in the discussion communication strategies and what kinds of creative strategies you will adopt to achieve this outcome.

Response Guidelines

Respond to at least one other learner and indicate what you like or dislike about their approach to selling organizational information security policies.

Course Resources
Undergraduate Discussion Participation Scoring Guide

Unit 9 >> Business Continuity Management Policy

Introduction

Business Continuity Planning is an activity that involves the entire organization. One of the most critical components of an organization is the data that is used to run the business and the equipment that supports it. This week you will focus on Technical Contingency Planning, which involves documenting and developing

recovery plans for IT hardware, software, and data. The technical contingency plan is considered a component of an overall business continuity plan.

Policies are only as effective as the communication and enforcement plan that supports them. This week you will discuss some strategies to ensure that the policies you develop and implement are enforced in a fair and consistent manner. You will also be asked to discuss some of the ramifications of not applying policies effectively.

Learning Activities

u09s1 - Studies

Your reading material for this unit covers concepts related to business continuity management, which is also the focus for the Unit 9 assignment and discussion.

Readings

Use the Capella Library to complete the following:

- In Stewart, Chapple, & Gibson's 2012 book, *CISSP: Certified Information Systems Security Professional Study Guide*,
  - Read Chapter 15, "Business Continuity Planning," pages 617–642.
- In Engemann & Henderson's 2012 book, *Business Continuity and Risk Management: Essentials of Organizational Resilience*,
  - Read Chapter 1, "Fundamentals of Business Continuity Managementm," pages 3– 14.
  - Read Chapter 2, "Business Continuity Management Organization," pages 15 – 20.
  - Chapter 10, "Business Continuity Plan," pages 123–138.
- Tammineedi's 2010 article, "Business Continuity Management: A Standards-Based Approach" from *Information Security Journal: A Global Perspective*, volume 19, issue 1, pages 36–50.

u09a1 - Business Continuity Management Policy

Using the resources provided and the project description, complete the policy template that you created in Unit 3 to draft a business continuity management policy appropriate to cover the functional areas related to operational management for the project organization.

Ensure that the following information is covered in the policy language proposed:

- Factors that are included within the scope and range of a business continuity management policy.
- Roles and responsibilities that are involved with the various activities included in the policies.
- Application of contextual characteristics specific to the project organization.
- Policy noncompliance procedures and penalties.

When complete, submit your document in the assignment area.

u09d1 - Policy Enforcement

You are the CIO for an organization that has an old idle policy manual on a shelf somewhere that governs the use of e-mail. All of the existing staff members were asked to read through the policy manual during their first week of service, but it is commonly known throughout the organization that no one really takes the time to do that.

Sally, who works on the IT support desk, receives a suggestive e-mail that she finds amusing. She forwards this e-mail to a Joe who works on the loading dock. Joe intends to send it to his friend Paul in the records department, but he selects instead a mailing list and the message is broadcast to the entire organization.

Paul's supervisor gets flooded with phone calls regarding the message and is so amused about the entire episode that he spends the day having a good laugh with his co-workers. Joe's supervisor is not so amused and gives Joe a 3 day unpaid suspension for distribution of the original e-mail. What will you, as CIO, do both in response to Sally's role in this as well as to address the inconsistent enforcement of policy going on within the other two departments?

Include in the discussion the role that consistent enforcement plays in the success of a policy development plan and strategies that can be used to increase the level of consistency within the organization.

Also, discuss the impact of inconsistent application of policy in the event that an employee who has been punished chooses to file legal action against the organization as a result of this policy enforcement.

Response Guidelines

Respond to at least one other learner who has taken a position different than your own and share why you believe your approach is more effective.

Course Resources
Undergraduate Discussion Participation Scoring Guide

Unit 10 >> IT and Technical Contingency Planning

Introduction

This week you will have an opportunity to review the materials you have covered in the course. You will be asked to finalize a set of policy recommendations for your project organization and to evaluate how these policies impact or support your work on risk assessment and business continuity planning for this organization.

Finally, you will be asked to share your insights into the material you have covered in the course and how the course may benefit you professionally.

Learning Activities

u10s1 - Studies

The readings below cover contigency and technical contingency planning concepts, which are also the focus of the Unit 10 assignment.

Readings

in Contingency Planning Guide for Information Technology Systems (NIST SP800-34), read the following. (This publication will be referred to as NIST SP800-34 for the remainder of this course.)

- Section 1, "Introduction," through Section 3.1, "Develop Contingency Planning Policy Statement."
- Section 3.2, "Conduct Business Impact Analysis" pages 16–18, and the information in Appendix B: Sample Business Impact Analysis and Business Impact Analysis Template, pages B-1–B-5.
- Section 3.4, "Develop Recovery Strategies," pages 18–27.
- Section 4, "IT Contingency Plan Development," pages 31–39.
- Section 5, "Technical Contingency Planning Considerations," pages 41–66.

u10a1 - IT Contingency and Technical Contingency Plans

Using the resources provided and the project description create and submit IT contingency and technical contingency plans for your project organization.

The plans should cover:

- Each of the five phases identified in Figure 4.1 – Contingency Plan Structure on page 31 of NIST SP800-34.
- All of the areas identified on page 41 of the NIST SP800-34 reference.
- The five common considerations and the IT platforms.

When complete, submit your documents in the assignment area.

Course Resources
Risk Assessment Documentation spreadsheet
Risk Impact Matrix
Business Impact Analysis Template

u10d1 - Record Management and Retention

Imagine that you have been hired by a federal agency to recommend implementation of a records management and retention process. This is your first job that involves working with records management and retention rules. Discuss the individual tasks that you think would be appropriate to include in this area of responsibility. Also discuss the general rules for electronic record management and retention. Include in the discussion some of the pros and cons of instituting a formal record management process and implementation plan, including tools and resources that you think may be useful in supporting the work.

Response Guidelines

Post your statement and support. Respond to one other learner. How well does the learner support his or her position? What evidence is the learner missing?

Course Resources
Undergraduate Discussion Participation Scoring Guide