Preview: ISTM5112 : Global Network Policy, Regulation, and Governance

Syllabus

Course Overview

In this course, you will explore different compliance laws and examine the impact of laws and regulations on information technology (IT) systems. You will strengthen your understanding and practice of risk assessment and network policies that mitigate risks and analyze methods of aligning these policies with business needs within the context of policies, laws, and regulations. This course also enables you to plan for contingencies in response to policy and regulatory change as well for U.S.-based businesses with global presence.

You will research many real-life enterprises to study the effect of compliance laws on the operation and identify the effect of negligence to the compliance laws through different scenarios. You will also discuss how to incorporate compliance in the risk assessment, mitigation, and auditing process.

You will be able to explain the laws and rules concerning encryption software, identify the laws that govern digital rights management, and explore ethical issues associated with information security. You will analyze global regulatory issues that impact U.S.-based systems with international presence and hypothesize the potential regulatory impact of an international political situation.

Finally, you will create information security policy for a global U.S.-based corporation (a fictitious enterprise) to model compliance with U.S. laws as well as international laws.

Course Competencies

(Read Only)

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

1. Apply risk assessment and risk modeling strategies.
2. Develop network policies to manage and mitigate risk.
3. Evaluate the legal impact of regulation on network operations.
4. Align network policies with strategic business plans and government regulations.
5. Plan for contingencies in response to political and regulatory change.

Course Prerequisites

Prerequisite(s): ITEC5060.

Syllabus >> Course Materials

Required

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

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.

- Adu, P. G., & Ward, K. W. (2011). Applying traditional risk assessment models to information assurance: A new domain not a new paradigm. *Review of Management Innovation & Creativity, 4*(11), 1–9.
- Blodgett, M. S. (2011). Substantive ethics: Integrating law and ethics in corporate ethics programs. *Journal of Business Ethics, 99*(Supplement 1), 39–48.
- Blythe, S. E. (2006). Cyberlaw of Japan: Promoting e-commerce security, increasing personal information confidentiality, and controlling computer access. *Journal of Internet Law, 10*(1), 20–26.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–A7.
- Ciurea, C. (2010). The informatics audit – A collaborative process. *Informatica Economica, 14*(1), 119–127.
- Cooper, T., Faseruk, A., & Johnson, L. D. (2010). Impact of privacy and confidentiality on valuation: An international perspective. *Journal of Financial Management & Analysis, 23*(2), 1–11.
- de Villiers, M. (2010). Information security standards and liability. *Journal of Internet Law, 13*(7), 24–33.
- Duska, R. F. (2011). Those darn compliance rules. *Journal of Financial Service Professionals, 65*(5), 22–24.
- Frenkel, D. A., & Lurie, Y. (2001). Electronic signature: Moral problems and the answer given by Israeli law. *EBS Review,* (13), 67–71.
- Gerber, M., & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security, 27*(5–6), 124–135.
- Green, I., Raz, T., & Zviran, M. (2007). Analysis of active intrusion prevention data for predicting hostile activity in computer networks. *Communications of the ACM, 50*(4), 63–68.
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236.

- Haber, E. M., Kandogan, E., & Maglio, P. P. (2011). Collaboration in system administration. *Communications of the ACM, 54*(1), 46–53.
- Healy, T. R., & Duke, K. E. (2002). Winners and losers under China's e-sign law. *China Business Review, 29*(6), 32.
- Henry, M. H., & Haimes, Y. Y. (2009). A comprehensive network security risk model for process control networks. *Risk Analysis: An International Journal, 29*(2), 223–248.
- Ion, I., Traian, S., & Cristian, A. (2008). The IT audit – A major requirement for the management quality and success in the European business context. *Annals of the University of Oradea, Economic Science Series, 17*(4), 1397–1401.
- Irion, K. (2009). Privacy and security: International communications surveillance. *Communications of the ACM, 52*(2), 26–28.
- Jiangping, W., & Lianyu, L. (2012). Risk management of IT service management project implementation with killer assumptions. *Technology & Investment, 3*(1), 48–55.
- Kim, S., Ullrich, J. B., & Wang, Q. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66–73.
- Lindenmayer, G. (2007). Information security standards: The 10 keys to protecting your network. *Risk Management, 54*(12), 11.
- Norman, W. (2011). Business ethics as self-regulation: Why principles that ground regulations should be used to ground beyond-compliance norms as well. *Journal of Business Ethics, 102*(Supplement 1), 43–57.
- Pagnattaro, M., & Peirce, E. R. (2007). Between a rock and a hard place: The conflict between U.S. corporate codes of conduct and European privacy and work laws. *Berkeley Journal of Employment & Labor Law, 28*(2), 375–428.
- Qing, H., Zhengchuan, X., Tamara, D., & Hong, L. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54–60.
- Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM, 49*(8), 97–100.
- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–A12.
- Suduc, A-M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica, 14*(1), 43–48.
- Teilans, A., Romanovs, A., Merkuryev, Y., Kleins, A., Dorogovs, P., & Krasts, O. (2011). Functional modelling of IT risk assessment support system. *Economics & Management, 16*, 1061–1068.
- Tribunella, T. J., & Tribunella, H. R. (2007). Ethics and security under the Sarbanes-Oxley Act. In M. Quigley (Ed.), *Encyclopedia of Information Ethics and Security (pp. 254 – 259)*. Gale Virtual Reference Library.
- Walker, R. S. (2004). The effect of recent US legislation and rule making on corporate compliance and ethics programmes. *International Journal of Disclosure & Governance, 1*(2), 138–145.

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.

- DSMSystems. (n.d.). Network security architecture – Part 1 [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=Lo-bfBUUyVs
- Grabowski, M. (2014, April 8). Internet law [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=0jDcgC8Zs2E
- Introduction to Risk Assessment [Video] | Transcript. (2010, October 11). null Retrieved from https://www.youtube.com/watch?v=EWdfovZlg2g
- IU Statewide IT Conference. (n.d.). Internal audit; Top ten IT audit findings and possible solutions [Video]. Retrieved from https://www.youtube.com/watch?v=GK6jZKqrjO8
- Meyers, J. (n.d.). Disaster recovery planning for IT [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=6nycHnHubZc
- Soper, D. (n.d.). Introduction to computer security – Information security lesson 1 of 12[Video]. Retrieved from https://www.youtube.com/watch?v=zBFB34YGK1U
- TEDxColumbus. (2013, October). The 1s and 0s behind cyber warfare [Video]. Retrieved from http://www.ted.com/talks/chris_domas_the_1s_and_0s_behind_cyber_warfare
- TEDxMaui. (2012, April 9). Jeremiah Grossman – Hack yourself first [Video] | Transcript. Retrieved from https://www.youtube.com/watch?v=-H2G2tlqSSM
- TEDxMidwest. (n.d.). Top hacker shows us how it's done – Pablos Holman [Video]. Retrieved from https://www.youtube.com/watch?v=hqKafl7Amd8
- TEDxPSU. (n.d.). Bruce Schneier – Reconceptualizing security [Video]. Retrieved from https://www.youtube.com/watch?v=CGd_M_CpeDI

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 readings may be available in the Capella University Library. 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. If the full text is not available, you may be able to request a copy through the Interlibrary Loan service.

- Lachance, D. (2015). CISSP: Network security and vulnerability management [Video]. Skillsoft Ireland.

- Shannon, M. (2016). CISA: Internet threats and security [Video]. Skillsoft Ireland.
- Skillsoft. (n.d.). CISSP: Security operations part 1 [Tutorial].
- Skillsoft. (n.d.). CompTIA Security+ SYO-401: Continuity, disaster recovery, and computer forensics [Tutorial].
- Skillsoft. (n.d.). CompTIA Security+ SYO-401: Creating secure networks [Tutorial].
- Skillsoft. (n.d.). CompTIA Security+ SYO-401: Network protocols, attacks, and defenses [Tutorial].

Projects

Project >> Security Policy

Project Overview

You have been asked to create a complete, comprehensive security policy for Honeycrisp Computers, and all but four sections have been completed.

The Final Paper Security Policy reflects the work that has already been completed, and that work has been finalized. **Note**: No changes should be made to the existing work.

Your task is to develop the remaining sections of the Security Policy, which are:

III. Risk Management.
V. Information Security Responsibilities.
VIII. Compliance.
IX. Password Control Standards.

Note: For this final assignment, develop the four remaining components and seamlessly implement that information into the existing policy. When finished, it should reflect one comprehensive, professional document.

Refer to all previous assignments, readings, and research to develop the missing components. To be comprehensive, make sure you thoroughly examine every scenario in its capacity to meet existing operations. Your policy components should clearly reflect this thorough examination.

In this project, you will be expected to:

- Develop a comprehensive compliance component for a security policy.
- Develop a comprehensive risk management component for a security policy.
- Develop comprehensive password control standards for a security policy.
- Develop comprehensive information security responsibilities for a security policy.

Your contribution should be 8 pages in length, which is roughly 2 pages per component.

- **Written communication**: Written communication is free of errors that detract from the overall message.
- **APA formatting**: Resources and citations are formatted according to APA sixth edition style and formatting guidelines.

- **Length of your contribution to the Final Paper Security Policy**: 8 typed, double-spaced pages.
- **Font and font size**: Times New Roman, 12 point.

Unit 1 >> Is Security a Must?

Introduction

Information is a person's private data, a company's intellectual property, or a country's national security interest. Information systems include hardware, operating system software, and applications that make up a system to provide access to information. Corporations and other entities must comply with a number of U.S. and international regulations related to data and privacy. More focus on compliance means more focus on information security, driving the demand for security professionals.

In this unit, you will categorize domains of a typical IT infrastructure and differentiate threats and risks to an IT system. You will also analyze the types of data classification standards.

In this unit, you will be presented with a list of some risks and threats associated with the seven domains of a typical IT infrastructure and you will be able to identify the preventive action for each.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *How Much Do We Know About Security?* Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

Course Resources

How Much Do We Know About Security?

Learning Activities

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *How Much Do We Know About Security?,* given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About Security?** to launch the quiz.

Readings

Use the Capella University Library to read Guo, Yuan, Archer, and Connelly's 2011 article, "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," from *Journal of Management Information Systems*, volume 28, issue 2, pages 203–236.

This reading will inform this unit's discussion as well as the Unit 2 assignment.

Internet Media

Click the link provided below to view the following Internet media piece:

- Introduction to Computer Security – Information Security Lesson 1 of 12 (transcript available via link).
  - This media piece will provide foundational context for your unit instruction.
  - Running time: 41:46.

Unit Research

In addition to the readings above, dedicate 1 hour to personal research. This research will be used in this unit's discussion and the Unit 2 assignment, as well as in your final project due in Unit 10.

Your research should be focused on categorizing the domains of a typical IT infrastructure in order to differentiate threats and risks to an IT system. You should also research the analysis of the types of data classification standards.

You can use the library to conduct your research. Also, you should consider the article given below. If you choose to view this article, type the title in the Search field, and then make sure the title, author, and date are accurate.

- Brenner, J. F. (2010). Privacy and security: Why isn't cyberspace more secure? *Communications of the ACM, 53*(11), 33–35.

Capella Media

Click **Risks and Threats** to view the media. After completing the unit discussion, complete this media piece. In this ungraded media piece, you will match IT risks and threats with possible solutions. This media piece will

inform your Unit 2 assignment as well as your final project.

Optional

Skillsoft Resources

- Skillsoft. (n.d.). CompTIA Security+ SYO-401: Network protocols, attacks, and defenses [Tutorial].
- Shannon, M. (2016). CISA: Internet threats and security [Video]. Skillsoft Ireland.

Course Resources
How Much Do We Know About Security?
Risks and Threats

u01d1 - Confidentiality

An acceptable use policy (AUP) is part of a layered approach to security and it supports confidentiality. In your opinion, what are the other standards that support confidentiality? Research a real-life scenario to support your opinion about other standards and how they support confidentiality. Through your research, did AUP contribute more to confidentiality than the other standards you researched?

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Introduction

A standard is an established and proven norm or method, which can be procedural or technical. A policy is a document that states how an organization is to perform and conduct business functions. On the other hand, a law is a collection or system of rules imposed by authority.

In this unit, you will explore many U.S. compliance laws. You will discuss Children's Internet Protection Act (CIPA) requirements, school disclosure exceptions in FERPA, directory information security in Federal Information Security Management Act (FISMA), the Gramm-Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HITECH Act, and the Sarbanes-Oxley (SOX) act.

You will also discuss the U.S. regulators, including Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), U.S. Department of Education, Department of Health and Human Services, and Office of Management and Budget. You will also evaluate recent legislation and industry standards that may impact network operations, analyze the effects of a regulation on IT systems, and describe the impacts of regulatory compliances on staffing and budgeting.

Finally, when your studies are complete, you will write a paper describing real-world implementations of U.S. compliance laws in both public and private sectors.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *How Much Do We Know About U.S. Compliance Laws?* Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

Course Resources
How Much Do We Know About U.S. Compliance Laws?

Learning Activities

u02s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *How Much Do We Know About U.S. Compliance Laws?*, given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded

quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

- Click **How Much Do We Know About U.S. Compliance Laws?** to launch the quiz.

Internet Media

Click the link provided below to view the following Internet media piece:

- Internet Law | Transcript.
  - This media piece will provide foundational context for your unit instruction.
  - Running time: 23:36.

Unit Research

In addition to the readings above, dedicate 1.5 hours to personal research. This research will be used in this unit's discussion and assignment, as well as in your final project.

In this unit, your research should be focused on evaluating recent legislation and industry standards that may impact network operations. You should also research the effects of a regulation on IT systems as a way to explain the impacts of regulatory compliances on staffing and budgeting.

Also, go to the Sarbanes-Oxley site. Sarbanes-Oxley is a financial law that is applicable to numerous fields. Bookmark this site, and use it as a resource throughout the course. This site is a simple and effective tool for understanding this law.

Research your area of interest or expertise in this site. Make note of your findings, and be sure to use them in your papers throughout the course.

You can use the library to conduct further research. Also, you should consider the articles below. If you choose to view these articles, type the titles in the Search field, and then make sure the title, author, and date are accurate.

- Duska, R. F. (2011). Those darn compliance rules. *Journal of Financial Service Professionals, 65*(5), 22–24.
- Tribunella, T. J., & Tribunella, H. R. (2007). Ethics and security under the Sarbanes-Oxley Act. In M. Quigley (Ed.), *Encyclopedia of Information Ethics and Security* (pp. 254 – 259). Gale Virtual Reference Library.

Course Resources

How Much Do We Know About U.S. Compliance Laws?

Below is a list of U.S. compliance laws. Select two laws that most pertain to your personal interest or experience. Explain the real-world applications of each law for *both* the public and private sectors. How does each law affect the organization?

Provide validation and support for arguments and ideas by incorporating relevant examples and supporting evidence from your research and readings in Unit 1 and this unit.

- Children's Internet Protection Act (CIPA).
- Family Educational Rights and Privacy Act (FERPA).
- Federal Information Security Management Act (FISMA).
- Gramm-Leach-Bliley Act (GLBA).
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Sarbanes-Oxley (SOX) Act.

In this paper, you are expected to:

- Analyze U.S. compliance laws to determine which best apply to a selected context.
- Apply compliance of the law as it applies to the selected *real-world* public context.
- Apply compliance of the law as it applies to the selected *real-world* private context.
- Provide validation and support for arguments and ideas by citing relevant examples and supporting evidence.
- Use proper essay format, grammar, punctuation, and APA references.

Note: Remember to cite your sources using APA sixth edition style and formatting. Your paper should be concise, well-organized, and 3–5 pages in length.

Before you begin, consult the U.S. Compliance Laws Scoring Guide to clarify the expectations for this assignment.

Course Resources

APA Style and Format

u02d1 - Protected Health Information Under HIPAA

Examine multiple examples (of different scope) of protected health information under HIPAA. Discuss one of the examples identified in detail and explain why it is protected by HIPAA. Research a real-life scenario to support

the examples you identified, and discuss the effect of your identified example and consequences in case of negligence.

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 3 >> Impact of Compliance Laws in Business

Introduction

In this unit, you will identify the types of disaster recovery plan tests, calculate the annual estimated loss due to a specific realized threat, and explain the step in a risk management process.

You will gather data and then enter it into standard formulas. The results can help you identify the priority of risks. You can also use the results to determine the effectiveness of controls. The risk occurs when a threat exploits vulnerability. You can use a scale to define the probability that a risk will occur. The scale can be based on word values such as *low*, *medium*, or *high*. You can then assign percentage values to these words. For example, you could assign a value of 10 percent to a low probability. You could assign 100 percent to a high probability.

Impact is used to identify the magnitude of a risk. The risk results in some type of loss. However, instead of quantifying the loss as a dollar amount, an impact assessment could use words such as *low*, *medium*, or *high*. You may also use these categories to identify probabilities. However, where a probability is expressed as a percentage, impact is expressed as a relative value. For example, *low* could be 10, *medium* could be 50, and *high* could be 100.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *How Much Do We Know About Business Law*? Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

Course Resources

How Much Do We Know About Business Law?

Learning Activities

u03s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *How Much Do We Know About Business Law?*, given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About Business Law?** to launch the quiz.

Readings

Use the library to read Norman's 2011 article, "Business Ethics as Self-Regulation: Why Principles That Ground Regulations Should Be Used to Ground Beyond-Compliance Norms as Well," from *Journal of Business Ethics*, volume 102, supplement 1, pages 43–57.

This reading will inform this unit's discussion as well as the Unit 4 assignment.

Internet Media

Click the link provided below to view the following Internet media piece:

- Disaster Recovery Planning for IT | Transcript.
  - This media piece will provide foundational context for your unit instruction.
  - Running time:10:13.

Unit Research

In addition to the readings above, dedicate 1 hour to personal research. This research will also be used in this unit's discussion and the Unit 4 assignment, as well as in your final project.

In this unit, your research should be focused on the types of disaster recovery plan tests, as well as calculating the annual estimated loss due to a specific realized threat. This research should help explain the steps in a risk management process.

You can use the library to conduct your research. Also, you should consider the articles below. If you choose to view these articles, type the titles in the Search field, and then make sure the title, author, and date are accurate.

- Walker, R. S. (2004). The effect of recent US legislation and rule making on corporate compliance and ethics programmes. *International Journal of Disclosure & Governance, 1*(2), 138–145.
- Blodgett, M. S. (2011). Substantive ethics: Integrating law and ethics in corporate ethics programs. *Journal of Business Ethics, 99*(Supplement 1), 39–48.

Capella Media

Click **The Impact of Laws** to view the media. After completing the unit discussion, complete this media piece. In this ungraded piece, you will explore the use of the laws: CIPA, FERPA, FISMA, GLBA, HIPAA, and SOX Act. This media piece will inform your Unit 4 assignment as well as your final project.

Course Resources
How Much Do We Know About Business Law?
The Impact of Laws

u03d1 - Disaster Recovery Plan Test

Analyze one of the types of disaster recovery plan tests. What are the methods of analysis? What is the goal of the analysis? Research a scenario when an enterprise failed to test the disaster recovery plan, and discuss how that enterprise was affected.

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Introduction

Governance involves specific actions an organization takes to ensure compliance with its policies, standards, baselines, procedures, and guidelines. Operational deviation from policy is not a problem when a solid business reason exists. However, as the number of exceptions grows, the policy's credibility is potentially reduced. Security policies are put in place to reduce risk.

Top-secret data refers to data whose unauthorized disclosure would reasonably be expected to cause grave damage to the national security. Secret data refers to data whose unauthorized disclosure would reasonably be expected to cause serious damage to the national security. Confidential data refers to data whose unauthorized disclosure would reasonably be expected to cause damage to the national security. Any military data that is considered *classified* must use one of these three classification levels. There is also unclassified data that is handled by government agencies.

In this unit, you will explain risk assessment methodologies, analyze potential threats to IT systems, and assess risks using quantitative and qualitative methods.

In this unit's assignment, you will be asked to assess a given security policy framework and identify its missing components. Then, you will write the access control standards and the password control standards sections of the security policy.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *HowMuch Do We KnowAbout IT in Business*? Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

Course Resources
How Much Do We Know About IT in Business?

Learning Activities

u04s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *How Much Do We Know About IT in Business?*, given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About IT in Business?** to launch the quiz.

Readings

Use the library to read Haber, Kandogan, and Maglio's 2011 article, "Collaboration in System Administration," from *Communications of the ACM*, volume 54, issue 1, pages 46–53.

This reading will inform this unit's discussion as well as assignment.

Internet Media

Click the link provided below to view the following Internet media piece:

- Introduction to Risk Assessment | Transcript.
- This media piece will provide foundational context for your unit instruction.
- Running time: 57:17.

Unit Research

In addition to the readings above, dedicate 1.5 hours to personal research. This research will be used in this unit's discussion and assignment, as well as in your final project.

In this unit, your research should be focused on risk assessment methodologies and the analysis of potential threats to IT systems. You should research both quantitative and qualitative methods.

You can use the library to conduct your research. Also, you should consider the articles below. If you choose to view these articles, type the titles in the Search field, and then make sure the title, author, and date are accurate.

- Qing, H., Zhengchuan, X., Tamara, D., & Hong, L. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM, 54*(6), 54–60.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–A7.
- Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–A12.

Course Resources

How Much Do We Know About IT in Business?

u04a1 - Remote Access Control Policy

For this assignment, you will play the role of an intern at Honeycrisp Computers, Inc. In one of your tasks, you have recently developed a design for a remote access control policy that indicated access controls for systems, applications, and data access. However, the senior network administrator would like you to get even more familiar with the company's complete IT security policy framework.

Using the illustration given in the Resources, which depicts a portion of the company's policy framework, examine the existing policy. Then, determine which components are missing from this security policy framework. Once determined, complete the policy by writing both the access control standards and the password control standards sections of the security policy.

In this paper, you will be expected to:

- Apply qualitative and quantitative risk assessment methodologies to a security policy.
- Analyze potential risks to an existing IT system.
- Propose effective solutions to identified risks.
- Provide validation and support for arguments and ideas by citing relevant examples and supporting evidence.
- Use proper essay format, grammar, punctuation, and APA references.

Incorporate examples from your research and readings in Unit 3 and this unit, to include both quantitative and qualitative risk management.

Remember to cite your sources using APA sixth edition style and formatting guidelines. Your paper should be concise, well-organized, and 3–5 pages in length.

Before you begin, consult the Remote Access Control Policy Scoring Guide to clarify the expectations for this assignment.

Course Resources

APA Style and Format

Remote Access Control Policy

u04d1 - Access to Classified Data

Explain how you would determine the appropriate access to classified data. Create an argument with a colleague, questioning your thought process of determining the appropriate access to classified data. Create a fictitious example to demonstrate your thought process to the management, and discuss holistically the financial benefit of your plan.

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 5 >> Check, Audit, and Test

Introduction

While you can test how administrators and mechanisms respond to a security incident with an audit, the methods used to exploit a vulnerability come from a security assessment. An audit will verify that you have taken adequate measures to protect sensitive data. An assessment will validate weaknesses that are not addressed by policy. Ethical hacking helps expose and prove inherent weaknesses that must be addressed by administrators and security professionals. Audits and assessments are performed in large organizations by dedicated teams, but smaller organizations may lack the resources.

Firewalls are excellent for restricting traffic but cannot distinguish between benign and malicious forms of permissible traffic. Firewall rules do not distinguish between legitimate traffic used in an illegitimate way or identify attack patterns in traffic.

In this unit, you will explain the process for verifying policy compliance, describe the process of monitoring a system for anomalies, as well as examine the drawbacks of log monitoring.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *HowMuch Do We KnowAbout Audit?* Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

Course Resources

How Much Do We Know About Audit?

Learning Activities

u05s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *HowMuch Do We KnowAbout Audit?*, given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About Audit?** to launch the quiz.

Readings

Use the library to read Suduc, Bîzoi, and Filip's 2010 article, "Audit for Information Systems Security," from *Informatica Economica*, volume 14, issue 1, pages 43–48.

This reading will inform this unit's discussion as well as Unit 6 assignment.

Internet Media

Click the link provided below to view the following Internet media piece:

- Internal Audit; Top Ten IT Audit Findings and Possible Solutions (Transcript available via link.)
  - This media piece will provide foundational context for your unit instruction.
  - Running time: 44:08.

Unit Research

In addition to the readings above, dedicate 2 hours to personal research. This research will be used in this unit's discussion and the Unit 6 assignment, as well as in your final project.

In this unit, your research should be focused on the process for verifying policy compliance to explain the process of monitoring a system for anomalies. You should also research the drawbacks of log monitoring.

You can use the library to conduct your research. Also, you should consider the articles below. If you choose to view these articles, type the titles in the Search field, and then make sure the title, author, and date are accurate.

- Ion, I., Traian, S., & Cristian, A. (2008). The IT audit – A major requirement for the management quality and success in the European business context. *Annals of the University of Oradea, Economic Science Series, 17*(4), 1397–1401.
- Ciurea, C. (2010). The informatics audit – A collaborative process. *Informatica Economica, 14*(1), 119–127.

Capella Media

Click **IT Roles** to view the media.

Click **Auditing System** to view the media.

After completing the unit discussion, complete these ungraded media pieces. In *IT Roles*, you will match IT roles with descriptions. In *Auditing System*, you will be asked to use the six steps of auditing system policies. These media pieces will inform your Unit 6 assignment as well as your final project.

Course Resources
How Much Do We Know About Audit?
IT Roles
Auditing System

u05d1 - Log Monitoring

Log monitoring provides a wealth of information and is considered one of the most important tools in tracing many aspects of a system. Log monitoring does have some drawbacks though. Discuss the drawbacks of log monitoring, and explain how to overcome any drawbacks. Research a real-life scenario where log monitoring caused issues to an enterprise, based on the drawbacks you identified.

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 6 >> Responding to Risk and Recovering

Introduction

When a threat exploits vulnerability, a risk occurs. Threats and vulnerabilities are identified as risks.

In this unit, you will identify the likelihood that a risk will occur. This can be based on historical data or opinions. For example, imagine a risk occurred at an average of six times in the past three years. If no steps are taken to reduce the risk, it will probably occur two times next year. If historical data is not available, experts can provide opinions on the likelihood of the risk occurring.

The value of assets helps to determine the impact of a risk. The assets can be hardware assets, software assets, or data. Some risks can affect all three.

Determining the value of assets can also be based on historical data or opinions. Imagine a risk resulted in losses averaging 20,000 dollars a year in the past three years. If no steps are taken to reduce the risk, it will probably result in a loss of about 20,000 dollars next year. If historical data is not available, experts can provide opinions on the impact of the risk.

In this unit, you will also determine the usefulness of a safeguard or control. Safeguards or controls are used to reduce the risk or reduce the impact. Some controls will be more effective than others. The risk assessment helps determine which ones to implement.

In this unit, you will describe the importance of managing risks to enterprise networks, assess threats and sources of threats to an IT system, and create security policy statements to mitigate specific risks.

Through this unit's assessment, you will answer the following questions:

- How to obtain a baseline of system or network behavior?
- What is an anomaly in relation to baseline behavior?

- Why might certain anomalies be worth investigating?
- How can traffic have patterns that signify known attacks?
- What do log files help you learn that filtering systems overlook?
- Why do legitimate traffic sometimes seem suspicious?

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *HowMuch Do We KnowAbout Risk?* Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

Course Resources

How Much Do We Know About Risk?

Learning Activities

u06s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *HowMuch Do We KnowAbout Risk?*, given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About Risk?** to launch the quiz.

Readings

Use the library to read Adu and Ward's 2011 article, "Applying Traditional Risk Assessment Models to Information Assurance: A New Domain Not a New Paradigm," from *Reviewof Management Innovation & Creativity*, volume 4, issue 11, pages 1–9.

This reading will inform this unit's discussion as well as assignment.

Internet Media

Click the link provided below to view the following Internet media piece:

- Top Hacker Shows Us How It's Done – Pablos Holman (transcript available via link).
  - This media piece will provide foundational context for your unit instruction.
  - Running time: 17:50.

Unit Research

In addition to the readings above, dedicate 2 hours to personal research. This research will be used in this unit's discussion and assignment, as well as in your final project.

In this unit, your research should be focused on explaining the importance of managing risks to enterprise networks and assessing threats and sources of threats to an IT system. You should also research the components that help create security policy statements to mitigate specific risks.

You can use the library to conduct your research. Also, you should consider the articles below. If you choose to view these articles, type the titles in the Search field, and then make sure the title, author, and date are accurate.

- Jiangping, W., & Lianyu, L. (2012). Risk management of IT service management project implementation with killer assumptions. *Technology & Investment, 3*(1), 48–55.
- Teilans, A., Romanovs, A., Merkuryev, Y., Kleins, A., Dorogovs, P., & Krasts, O. (2011). Functional modelling of IT risk assessment support system. *Economics & Management,* 16, 1061–1068.

Optional

Skillsoft Resources

- Skillsoft. (n.d.). CompTIA Security+ SYO-401: Continuity, disaster recovery, and computer forensics [Tutorial].

Course Resources

How Much Do We Know About Risk?

u06a1 - Security Events, Baselines, and Anomalies

Network endpoints and network devices have different security considerations and implications. A user workstation implies certain security issues that remain in the user domain, while network implications remain part of the LAN or LAN-to-WAN domain. However, during the course of investigating an intrusion, you may have to source data from logs kept in routing devices and end-user systems.

Suppose an attacker intrudes upon one of your servers, how do you reconstruct the events of a crime? Log files are the first place to check for administrative issues and security activity. Log files help you put together a timeline of events surrounding everything from a performance problem to a security incident.

You can also identify bad system or network activities by observing anomalies from baseline behavior or identifying certain suspicious actions. Testing ensures that your control and monitoring facilities work as intended and maintain proper operation. Monitoring ensures that you capture evidence when your testing procedures fail to examine all possibilities or when legitimate behavior permits unauthorized activity.

Always consider that even legitimate traffic can be used in illegitimate ways and, sometimes, legitimate traffic can appear illegitimate. Protected services can be attacked from the inside or accessed externally through loopholes in firewall rules. Vulnerabilities may remain unidentified by intrusion detection system (IDS) or intrusion prevention system (IPS) signatures and evade detection. Monitoring helps you capture pieces of the puzzle that creates a timeline of events.

Policy violations and security breaches take many forms, and not all of them are obvious. For example, you might have a policy that specifies a certain minimum password length, but fails to enforce proper complexity, allowing passwords to be easily guessed.

In this assignment, you will explain solutions for at least two significant types of security events and baseline anomalies that might indicate suspicious activity, in connection with your area of interest or experience.

Contemplate the following questions before completing this assignment:

- How do you obtain a baseline of system or network behavior?
- What is an anomaly in relation to baseline behavior?
- Why might certain anomalies be worth investigating?
- How can traffic have patterns that signify known attacks?
- What do log files help you learn that filtering systems overlook?
- Why do legitimate traffic sometimes seem suspicious?

In this paper, you will be expected to:

- Explain how irregularities in usability trends lead to security events.
- Explain how log files can be used to determine the legitimacy of irregular traffic trends.
- Propose solutions to security events and baseline anomalies.
- Provide validation and support for arguments and ideas by citing relevant examples and supporting evidence.
- Use proper essay format, grammar, punctuation, and APA references.

Remember to cite your sources (from your readings and research) using APA sixth edition style and formatting guidelines. Your paper should be concise, well-organized, and 3–5 pages in length. Before you begin, consult the Security Events, Baselines, and Anomalies Scoring Guide to clarify the expectations for this assignment.

Course Resources

APA Style and Format

u06d1 - Business Continuity Management

Examine the primary components of business continuity management (BCM) and discuss one of the primary components in detail. Make sure you address how this component affects BCM. Research a real-life situation where an enterprise neglected one of the identified primary components and discuss how that affected the continuity of the business.

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 7 >> Network Risks and Defense Tools

Introduction

In this unit, you will examine the tools required to properly assess the security architecture, examine the relationship of internal and external security to the security architecture, as well as analyze the mechanisms used to achieve a secure infrastructure.

You will examine the different layers of the very basic open systems interconnection (OSI) model as well as the functionalities and characteristics of each level. Then, you will dig deep into two of the most important components connecting the backbone of your network—routers and switches.

Given below is a refresher of the OSI network model.

OSI Network Model

Layer 1: Physical layer defines electrical and physical device specifications and relationships between physical devices. Ethernet cabling functions at this layer.

Layer 2: Data link layer provides the means to transfer data between network endpoints. Most switches operate at this layer.

Layer 3: Network layer provides means for delivering variable-length data between networks. Routers operate at this layer.

Layer 4: Transport layer establishes reliable services and uses connection- or datagram-oriented packets. Transmission control protocol (TCP) and user datagram protocol (UDP) exist at this layer.

Layer 5: Session layer establishes, manages, and terminates connections locally and remotely. Remote procedure calls (RPCs) function at this layer.

Layer 6: Presentation layer establishes context between application layer entities.

Layer 7: Application layer interacts with software that uses a communication protocol. It is closest to the end-user with direction application interaction. It serves to identify parties, determine service availability, and synchronize end-to-end communications. HTTP, FTP, and e-mail services all serve client functions at this level.

Switches transfer network connections at Layer 2, the lowest level of logical traffic flow (frames). Only specialized multi-layer switches operate at other layers.

Routers transfer network connections at Layer 3, where more routing features become available (packets). They are configurable to handle more complex routing tasks. Routers bridge internal and external connections alike, but switches primarily serve internal functions. They have greater exposure to external attacks and attackers.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *How Much Do We Know About Defense*? Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

Course Resources

How Much Do We Know About Defense?

Learning Activities

u07s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *How Much Do We Know About Defense?*, given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About Defense?** to launch the quiz.

Readings

Use the library to read Henry and Haimes's 2009 article, "A Comprehensive Network Security Risk Model for Process Control Networks," from *Risk Analysis: An International Journal*, volume 29, issue 2, pages 223–248.

This reading will inform this unit's discussion as well as the Unit 8 assignment.

Internet Media

Click the link provided below to view the following Internet media piece:

- Network Security Architecture – Part 1 | Transcript.
  - This media piece will provide foundational context for your unit instruction.
  - Running time: 11:01.

Unit Research

In addition to the readings above, dedicate 1.5 hours to personal research. This research will be used in this unit's discussion and the Unit 8 assignment, as well as in your final project.

In this unit, your research should be focused on acquiring the tools required to properly assess the security architecture, which will help explain the relationship of internal and external security to the security architecture. You should also research the mechanisms used to achieve a secure infrastructure.

You can use the library to conduct your research. Also, you should consider the articles below. If you choose to view this article, type the title in the Search field, and then make sure the title, author, and date are accurate.

- Green, I., Raz, T., & Zviran, M. (2007). Analysis of active intrusion prevention data for predicting hostile activity in computer networks. *Communications of the ACM, 50*(4), 63–68.

Capella Media

Click **Domains and A-I-C Functions** to view the media. After completing the unit discussion, complete the media piece. In this ungraded media piece, you will explore network security applications and countermeasures, domains, and I-C functions. This media piece will inform your Unit 8 assignment as well as your final project.

Optional

Skillsoft Resources

- Skillsoft. (n.d.). CompTIA Security+ SYO-401: Creating secure networks [Tutorial].
- Lachance, D. (2015). CISSP: Network security and vulnerability management [Video]. Skillsoft Ireland.

Course Resources
How Much Do We Know About Defense?
Domains and A-I-C Functions

u07d1 - Security Levels

Analyze the configurations to determine the best one for hosting a public Web site or your own e-mail server, for which you need to allow inbound connections on a limited basis. Make sure to use the configuration that is best for networks with varying security levels, such as general users, a group of users working on a secret research project, and a group of executives.

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 8 >> Standards of Information Security

Introduction

In this unit, you will explain the role of a policy in an enterprise networking context, explain the processes by which network policies are developed and analyzed to develop the foundations to create a network policy to support mission critical business processes, and examine real-world implementations of security standards.

Although the PCI DSS is not a law or government regulation, if a merchant is found not to be in compliance, hefty penalties can occur. On failing to meet the requirements of PCI DSS specifications, a mid-sized merchant who deals with 1–6 million dollars of credit card transactions annually could be fined thousands of dollars. From Visa, fines for a single month could accumulate to 25,000 dollars. If compliance is still not followed, payment brands that belong to the PCI Security Standards Council can remove the merchant's ability to make credit card transactions.

An auditor conducts a PCI DSS security assessment to determine whether a merchant is in compliance with the current data security standard. A qualified security assessor (QSA) is someone trained, licensed, and authorized by the PCI Security Standards Council to conduct a PCI DSS security assessment.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *How Much Do We Know About Standards*? Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

Course Resources
How Much Do We Know About Standards?

Learning Activities

u08s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *How Much Do We Know About Standards?*, given in the introduction to of this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About Standards?** to launch the quiz.

Readings

Use the library to read Siponen's 2006 article, "Information Security Standards Focus on the Existence of Process, Not Its Content," from *Communications of the ACM*, volume 49, issue 8, pages 97–100.

This reading will inform this unit's discussion as well as assignment.

Internet Media

Click the link provided below to view the following Internet media piece:

- Bruce Schneier – Reconceptualizing Security (transcript available via link).
  - This media piece will provide foundational context for your unit instruction.
  - Running time: 21:14.

Unit Research

In addition to the readings above, dedicate 1.5 hours to personal research. This research will also be used in this unit's discussion and assignment, as well as in your final project.

In this unit, your research should be focused on the role of a policy in an enterprise networking context, as well as the processes by which network policies are developed and analyzed to create a network policy to support mission critical business processes.

You can use the library to conduct your research. Also, you should consider the articles below. If you choose to view these articles, type the titles in the Search field, and then make sure the title, author, and date are accurate.

- de Villiers, M. (2010). Information security standards and liability. *Journal of Internet Law, 13*(7), 24–33.
- Lindenmayer, G. (2007). Information security standards: The 10 keys to protecting your network. *Risk Management, 54*(12), 11.

Optional

Skillsoft Resources

- Skillsoft. (n.d.). CISSP: Security operations part 1 [Tutorial].

Course Resources

How Much Do We Know About Standards?

In this paper, you will examine *real-world* applications of security standards.

Below is a list of international and U.S. standards organizations. Select two information security standards developed by these organizations that most pertain to your personal interest or experience. Explain the real-world applications of each standard for both the public and private sectors. How does each standard affect the organization?

Provide validation and support for arguments by incorporating relevant examples and supporting evidence from your research and readings in Unit 7 and this unit, to include mechanisms used in a security context.

Standards Organizations:

- American National Standards Institute (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE).
- International Electrotechnical Commission (IEC).
- International Organization for Standardization (ISO).
- International Telecommunication Union Telecommunication Sector (ITU-T).
- Internet Architecture Board (IAB).
- Internet Engineering Task Force (IETF).
- National Institute of Standards and Technology (NIST).
- Payment Card Industry's Data Security Standards (PCI DSS).
- World Wide Web Consortium (W3C).

In this paper, you are expected to:

- Apply security standards to the selected *real-world* public context.
- Apply security standards to the selected *real-world* private context.
- Explain mechanisms in the security context of an existing business.
- Provide validation and support for arguments and ideas by citing relevant examples and supporting evidence.
- Use proper essay format, grammar, punctuation, and APA references.

Note: Remember to cite your sources using APA sixth edition style and formatting guidelines. The paper should be well-organized and 3–5 pages in length.

Before you begin, consult the Security Standards Scoring Guide to clarify the expectations for this assignment.

Course Resources

APA Style and Format

u08d1 - RFC Designation

What are the formal stages or designation of an RFC? In your opinion, which one is the most important? Why? Do a research on a real-life situation, emphasizing the importance of the stage identified, and discuss the effect of ignoring that stage.

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 9 >> Global Compliance Laws and Regulations

Introduction

In this unit, you will explain the laws and rules concerning encryption software in the real world, analyze the laws that govern digital rights management, and then explore ethical issues associated with information security. You will also begin to research the area of privacy, which will also be addressed in Unit 10. These areas of study will be addressed in your final project.

According to Conklin, White, Williams, Davis, Cothren, and Schou (2009):

> Encryption technology has been controlled by governments for a variety of reasons. The level of control varies from outright banning to little or no regulation. The reasons behind the control vary as well, and control over import and export is a vital method of maintaining a level of control over encryption technology in general. The majority of the laws and restrictions are centered on the use of cryptography, which was until recently used mainly for military purposes.
>
> The advent of commercial transactions and network communications over public networks such as the Internet has expanded the use of cryptographic methods to include securing of network communications. As is the case in most rapidly changing technologies, the practice moves faster than law. Many countries still have laws that are outmoded in terms of e-commerce and the Internet. Over time, these laws will be changed to serve these new uses in a way consistent with each country's needs.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz, *How Much Do We Know About Global Compliance*? Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit.

References

Conklin, W. A., White, G., Williams, D., Davis, R., Cothren, C., & Schou, C. (2009). *Principles of computer security: CompTIA security+ and beyond* (2nd ed.). New York, NY: Mc-Graw-Hill.

Course Resources

How Much Do We Know About Global Compliance?

Learning Activities

u09s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *How Much Do We Know About Global Compliance?*, given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About Global Compliance?** to launch the quiz.

Readings

Use the library to complete the following:

- Read Gerber and von Solms's 2008 article, "Information Security Requirements – Interpreting the Legal Aspects," from *Computers & Security*, volume 27, issue 5–6, pages 124–135.
- Read Pagnattaro and Peirce's 2007 article, "Between a Rock and a Hard Place: The Conflict Between U.S. Corporate Codes of Conduct and European Privacy and Work Laws," from *Berkeley Journal of Employment & Labor Law*, volume 28, issue 2, pages 375–428.

These readings will inform this unit's discussion and the Unit 10 discussion, as well as your final paper.

Internet Media

Click the link provided below to view the following Internet media piece:

- Jeremiah Grossman – Hack Yourself First | Transcript.
  - This media piece will provide foundational context for your unit instruction.
  - Running time: 13:21.

Unit Research

In addition to the readings above, dedicate 2.25 hours to personal research. This research will be used in this unit's discussion and the Unit 10 discussion, as well as your final project.

In this unit, your research should be focused on the laws and rules concerning encryption software, as well as determining the laws that govern digital rights management. You should also explore ethical issues associated with information security.

In addition, your research should focus on the global regulatory issues that impact U.S.-based systems with international presence. Finally, explore the potential regulatory impact of an international political situation, which will help create information security policy for a global U.S.-based corporation.

You can use the library to conduct your research. Also, you should consider the articles below. If you choose to view these articles, type the titles in the Search field, and then make sure the title, author, and date are accurate.

- Kim, S., Ullrich, J. B., & Wang, Q. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66–73.
- Blythe, S. E. (2006). Cyberlaw of Japan: Promoting e-commerce security, increasing personal information confidentiality, and controlling computer access. *Journal of Internet Law, 10*(1), 20–26.
- Healy, T. R., & Duke, K. E. (2002). Winners and losers under China's e-sign law. *China Business Review, 29*(6), 32.
- Frenkel, D. A., & Lurie, Y. (2001). Electronic signature: Moral problems and the answer given by Israeli law. *EBS Review*, (13), 67–71.
- Cooper, T., Faseruk, A., & Johnson, L. D. (2010).Impact of privacy and confidentiality on valuation: An international perspective. *Journal of Financial Management & Analysis, 23*(2), 1–11.
- Irion, K. (2009). Privacy and security: International communications surveillance. *Communications of the ACM, 52*(2), 26–28.

Course Resources

How Much Do We Know About Global Compliance?

u09d1 - Ethical Aspects of Monitoring

The vice president of information security wants to monitor user actions on the company's intranet. What is the best method of obtaining the proper permissions? Research the ethical aspect of obtaining permission and examine both sides of the argument, emphasizing the reasons that support the side you are taking in the argument.

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide

Unit 10 >> A Global View on Privacy

Introduction

As the international and global market flourishes, many corporations have to establish relationships and, sometimes, even partnerships with countries overseas. In this unit, you will continue to analyze global regulatory issues that impact U.S.-based systems with international presence, analyze the potential regulatory impact of possible international political situations, as well as develop information security policy for a global U.S.-based corporation.

This information as well as the following information on privacy will be put to use in your final project.

According to Conklin, White, Williams, Davis, Cothren, and Schou (2009), privacy is not a U.S.-centric phenomenon, but it does have strong cultural biases. Legal protections for privacy tend to follow the socio-cultural norms by geography; hence, there are different policies in European nations than in the United States. In the United States, the primary path to privacy is via opt-out, whereas in Europe and other countries, it is via opt-in. What this means is that the fundamental nature of control shifts.

Conklin et al. also pointed out that in the U.S., a consumer must notify a firm that they wish to block the sharing of personal information; otherwise the firm has permission by default. In the EU, sharing is blocked unless the customer specifically opts in to allow it. The Far East has significantly different cultural norms with respect to individualism versus collectivism and this is seen in their privacy laws as well. Even in countries with common

borders, distinct differences exist, such as the United States and Canada; Canadian laws and customs have strong roots to their UK history, and in many cases follow European ideals as opposed to U.S. ones.

Conklin et al. further stated that one of the primary sources of intellectual and political thought on privacy has been the Organization for Economic Co-operation and Development (OECD). This multinational entity has for decades conducted multilateral discussions and policy formation on a wide range of topics, including privacy.

This information is a continuation of your readings about privacy from Unit 9, and you will incorporate many of these concepts in your final project, which is due at the end of this unit.

Pre-Assessment Quiz

Before you begin this unit, take the pre-assessment interactive quiz *How Much Do We Know About Privacy?* Click **Launch Presentation** to launch the quiz.

After taking this ungraded quiz, you should be aware of the knowledge and skills you already possess in regard to the topics that will be discussed in this unit. You may have acquired some of this content in Unit 9, so this quiz will demonstrate how much you have retained.

References

Conklin, W. A., White, G., Williams, D., Davis, R., Cothren, C., & Schou, C. (2009). *Principles of computer security: CompTIA security+ and beyond* (2nd ed.). New York, NY: Mc-Graw-Hill.

Course Resources

How Much Do We Know About Privacy?

Learning Activities

u10s1 - Studies

Pre-Assessment Quiz

You should have completed the pre-assessment quiz *How Much Do We Know About Privacy?*, given in the introduction to this unit. If not, complete this quiz before you begin any other unit tasks. This ungraded quiz is designed to not only inform you of what content will be addressed in this unit, but it will also make you aware of the knowledge and skills you already possess in regard to this topic.

Click **How Much Do We Know About Privacy?** to launch the quiz.

Internet Media

Click the link provided below to view the following Internet media piece:

- The 1s and 0s Behind Cyber Warfare (transcript available via link).
  - This media piece will provide foundational context for your unit instruction.
  - Running time: 16:41.

Readings and Research

There are no assigned readings and research for this unit. You should analyze and synthesize the information you gathered in the previous nine units to create the security policy components for your final paper.

Final Paper

You should commit 8 hours to the completion of your final paper. Review your previous research, organize your data, and then complete your paper.

Course Resources

How Much Do We Know About Privacy?

u10a1 - Security Policy

Submit your final project in the assignment area by the end of the week.

For clarification on project criteria, refer to Security Policy course project description.

Course Resources

APA Style and Format

u10d1 - Compliance Between U.S. and European Markets

What is the primary factor behind data-sharing compliance between U.S. and European companies? Research a real-life situation where international laws caused an enterprise to loosen its standards to accommodate a partner overseas. How did that accommodation affect the business of the enterprise?

Please cite the location of any example you use. Also, please feel free to use a fictitious enterprise as long as you can create a background of the fictitious enterprise to demonstrate your opinion.

Response Guidelines

Respond substantively to the post of at least one other learner.

Course Resources
Graduate Discussion Participation Scoring Guide