NYU SCHOOL OF PROFESSIONAL STUDIES

Information Security Management

MASY1-GC 3220 | 101 | Spring 2024 | 01/22/2024 -05/06/2024 | 3 Credit
Modality: In-person
Course Site URL: https://brightspace.nyu.edu

General Course Information

Name/Title: Arnold Louis Felberbaum / Adjunct Instructor
NYU Email: ALF380@nyu.edu
Class Meeting Schedule: 01/22/2024 - 05/06/2024 | Monday | 02:00pm -- 04:35pm
Class Location: 20 W 43rd St (Midtown Ctr) Room 524
Office Hours: Availability for an appointment on Monday, Tuesday, Thursday 11am-4pm EST/EDT via NYU Zoom days/times (please contact me via Email to arrange an appointment

Description

This course focuses on the importance of protecting data and information in today's digital world as related to strategy and policy, awareness, data classification, ownership and accountability, monitoring and reporting. The course covers network components that comprise the environment, where the data are input, processed, stored and how the data travel through the Intranet, Extranet, and/or Internet. Upon completion of the course, students learn to assess the impact of data in the digital world, considering the steps that the Government, Corporations and the Private Sector take to protect information assets. Students gain an understanding of components that comprise network security and how each component provides protection. They become familiar with preventative and detective tools such as anti-malware, ACL, virus protection, cryptography, intrusion detection, audit logs, and logical and physical controls and perform information risk assessments.

Prerequisites

1240 - Information Technology and Data Analytics

Learning Outcomes

At the conclusion of this course, students will be able to:

- Apply the key principles of information security to the value of data and technologies in the digital world
- Analyze different security frameworks used by Government, Corporations, and the Private Sector to protect digital asset
- Design a digitally secure environment to protect business information assets
- Justify how each digital security component provides protection from threats
- Support the decision to select and use preventive, detective, and responsive security elements
- Perform information security risk assessment to quantify and address high risk occurrences

Communication Methods

Be sure to turn on your NYU Brightspace notifications and frequently check the

"Announcements" section of the course site. This will be the primary method I use to communicate information critical to your success in the course. To contact me, send me an email. I will respond within 24 hours.

Structure | Method | Modality

There are 14 session topics in this course. The session topics are organized into three (3) areas of study: 1) Background Context, 2) Tools and Techniques, and 3) Application and Practices in Security.

Active learning experiences and small group projects are key components of the course. Assignments, papers, and exams will be based on course materials (e.g., readings, videos), lectures, and class discussions. Course sessions will be conducted synchronously on NYU Zoom, which you can access from the course site in NYU Brightspace.

Expectations

Learning Environment

You play an important role in creating and sustaining an intellectually rigorous and inclusive classroom culture. Respectful engagement, diverse thinking, and our lived experiences are central to this course, and enrich our learning community.

Participation

You are integral to the learning experience in this class. Be prepared to actively contribute to class activities, group discussions, and work outside of class.

Assignments and Deadlines

Please submit all assignments to the appropriate section of the course site in NYU Brightspace. If you require assistance, please contact me BEFORE the due date.

Course Technology Use

We will utilize multiple technologies to achieve the course goals. I expect you to use technology in ways that enhance the learning environment for all students.

Feedback and Viewing Grades

I will provide timely meaningful feedback on all your work via our course site in NYU Brightspace. You can access your grades on the course site Gradebook.

Attendance

I expect you to attend all class sessions. Attendance will be taken into consideration when determining your final grade. Refer to the SPS Policies and Procedures page for additional information about attendance.

Textbooks and Course Materials

Management of Information Security
ISBN: 978-1-337-40571-3
by Michael E. Whitman, Herbert J. Mattord

Available to Purchase or Rent on Amazon in print for $32.84 - $93.52, or digital eTextbook to rent for $49.49 or to buy for $86.49

Grading | Assessment

Your grade in this course is based on your performance on multiple activities and assignments. Since all graded assignments are related directly to course objectives and learning outcomes, failure to complete any assignment will result in an unsatisfactory course grade. All written assignments are to be completed using APA format and must be typed and double-spaced. Grammar, punctuation, and spelling will be considered in grading. Please carefully proof-read your written assignments before submitting them for a grade. I will update the grades on the course site each time a grading session has been completed— typically three (3) days following the completion of an activity.

DESCRIPTION	PERCENTAGE
Assigned team Activities (total of 12)	40%
Chapter Quizzes (total of 12)	20%
Participation	10%
Final Paper	30%
TOTAL POSSIBLE	100%

See the "Grades" section of Academic Policies for the complete grading policy, including the letter grade conversion, and the criteria for a grade of incomplete, taking a course on a pass/fail basis, and withdrawing from a course.

Course Outline

Start/End Dates: 01/22/2024 -05/06/2024 | Monday
Time: 02:00pm -- 04:35pm
No Class Date(s): Monday - 2/19/2024 and 03/18/2024
Special Notes: Spring Break 03/18/24 - 03/24/24

Session 1, 01/22/24
Introduction to the Management of Information Security

- Overview of Class Operation.
- Discuss the key characteristics of information security.
- Discuss the key characteristics of leadership and management.
- Describe the importance of the manager's role in securing an organization's information assets.
- Differentiate information security management from general business management.

Reading:

- Chapter 1

Deliverables:

- Review Class Guidelines
- Review Semester Deliverables
- Distribute team exercise due 01/29/2024 at 2:30
- Enable chapter questions due 01/29/2024 at 2:00

Session 2, 01/29/24
Implications of Compliance and Ethical Consideration

- Differentiate between law and ethics.
- Describe the ethical foundations and approaches that underlie modern codes of ethics.
- Discuss relevant professional organizations.
- Describe why ethical codes of conduct are important to InfoSec professionals and their organizations.

Examine the impact of AI on privacy.

Reading:

- Chapter 2

Deliverables:

- Review Team Exercise #1 Assignment
- Distribute team exercise due 02/05/2024 at 2:30
- Enable chapter questions due 02/05/2024 at 2:00

Session 3, 02/05/24
Governance and Strategic Planning for Managing Security

- Identify the key organizational stakeholders that are actively involved in planning and their roles.
- Discuss strategic organizational planning for information security (InfoSec)
- Define the importance, benefits, and outcomes of information security governance

Reading:

- Chapter 3

Deliverables:

- Review Team Exercise #2 Assignment
- Distribute team exercise due 02/12/2024 at 2:30
- Enable questions due 02/12/2024 at 2:00

Session 4, 02/12/24
Managing and Creating the Security Policy

- Define information security policy and discuss making them successful.
- Describe the major types of information security policy and discuss the major components of each.
- Discuss the process of developing, implementing, and maintaining various types of information security policies.

Reading:
- Chapter 4

Deliverables:
- Review Team Exercise #3 Assignment
- Distribute team exercise due 02/26/2024 at 2:30
- Enable questions due 02/26/2024 at 2:00

Session 5, 02/26/24
Managing the Security Program through Policy and Experience
- Identify the functional components of an information security program.
- Discuss how to plan and staff an organization's information security program.
- Review the internal and external factors that influence the activities and organization of an information security program.
- Discuss the components of a security education, training, and awareness program and explain how organizations create and manage these programs.
- Discuss the role of project management in information security.

Reading:
- Chapter 5

Deliverables:
- Review Team Exercise #4 Assignment
- Distribute team exercise due 003/04/2024 at 2:30
- Enable questions due 03/04/2024 at 2:00

Session 6, 03/04/24
Risk Management and Assessing the Risk
- Define risk management and its role in the organization.
- Describe risk management techniques to identify and prioritize risk factors for information assets.
- Explain how risk is assessed based on the likelihood of adverse events and the effects on information assets when events occur.
- Discuss the use of the results of the risk identification process.

Reading:
- Chapter 6

Deliverables:

- Review Team Exercise #5 Assignment
- Distribute team exercise due 03/11/2024 at 2:30
- Enable questions due 03/11/2024 at 2:00

Session 7, 03/11/24
Using Security to Treat Risk

- Identify the strategy options used to treat risk and be prepared to select from them when given background information.
- Evaluate control alternatives under the defense risk treatment strategy and formulate a cost-benefit analysis (CBA) using existing conceptual frameworks.
- Explain how to maintain and perpetuate controls.
- Common approaches used in industry to manage risk.

Reading:

- Chapter 7

Deliverables:

- Review Team Exercise #6 Assignment
- Distribute team exercise due 03/25/2024 at 2:30
- Enable questions due 03/25/2024 at 2:00

Session 8, 03/25/24
Security Management Models

- Describe the dominant InfoSec management models, including national and international standards-based models.
- Explain why access control is an essential element of InfoSec management.
- Recommend an InfoSec management model and explain how it can be customized to meet the needs of a particular organization.
- Describe the fundamental elements of key InfoSec management practices.

Reading:

- Chapter 8

Deliverables:

- Review Team Exercise #7 Assignment
- Distribute team exercise due 04/01/2024 at 2:30
- Enable questions due 04/01/2024 at 2:00

Session 9, 04/01/24

Security Management Practices

- Identify the elements of key information security management practices.
- Information security constraints on general hiring processes.
- Explain the role of information security in employee terminations.
- Describe the security practices used to regulate employee behavior and prevent misuse of information.
- Discuss the various types of benchmarking and their use in security planning.

Reading:

- Chapter 9

Deliverables:

- Review Team Exercise #8 Assignment
- Distribute team exercise due 04/08/2024 at 2:30
- Enable questions due 04/08/2024 at 2:00

Session 10, 04/08/24
Planning for Contingencies

- Discuss the need for contingency planning.
- Describe the major components of incident response, disaster recovery, and business continuity.
- Define the components of crisis management and business resumption.
- Discuss how the organization would prepare and execute a test of contingency plans.

Reading:

- Chapter 10

Deliverables:

- Review Team Exercise #9 Assignment
- Distribute team exercise due 04/15/2024 at 2:30
- Enable questions due 04/15/2024 at 2:00

Session 11, 04/15/24
Maintaining Security

- Discuss the need for ongoing maintenance of the information security program.
- Define a model for a maintenance program.
- Identify the key factors involved in monitoring the external and internal environment.
- Describe how planning, risk assessment, vulnerability assessment, and remediation tie into information security maintenance.
- Explain how to build readiness and review procedures into information security maintenance.

Reading:

- Chapter 11

Deliverables:
- Review Team Exercise #10 Assignment
- Distribute team exercise due 04/22/2024 at 2:30
- Enable questions due 04/22/2024 at 2:00

Session 12, 04/22/24
Protection Mechanisms
- Describe the various access control approaches, including authentication, authorization, and biometric access controls.
- List and discuss the various types of firewalls and the common approaches to firewall implementation.
- Define and describe the types of intrusion detection and prevention systems and the strategies on which they are based.
- Explain the unique challenges associated with physical security and discuss how physical security can supersede computer security.
- Explain cryptography and the encryption process and compare and contrast symmetric and asymmetric encryption.

Reading:
- Chapter 12

Deliverables:
- Review Team Exercise #11 Assignment
- Distribute team exercise due 04/19/2024 at 2:30
- Enable questions due 04/29/2024 at 2:00

Session 13, 04/29/24
Semester Review

Reading:
- Chapter 13

Deliverables:
- Review Team Exercise #12 Assignment
- Final Paper Deliverable Review

Session 14, 05/06/24
FINAL Presentations

Reading:

- Chapter 14

Deliverables:

Course Outline Table:

Date	Description	Chapter	Deliverables
Session 1 **01/22/2024**	**Introduction to the Management of Information Security** • Overview of Class Operation. • Discuss the key characteristics of information security. • Discuss the key characteristics of leadership and management. • Describe the importance of the manager's role in securing an organization's information assets. • Differentiate information security management from general business management.	1	Review Class Guidelines Review Semester Deliverables Distribute team exercise due 01/29/2024 at 2:30 Enable chapter questions due 01/29/2024 at 2:00
Session 2 **01/29/2024**	**Implications of Compliance and Ethical Consideration** • Differentiate between law and ethics. • Describe the ethical foundations and approaches that underlie modern codes of ethics. • Discuss relevant professional organizations. • Describe why ethical codes of conduct are important to InfoSec professionals and their organizations.	2	Review Team Exercise #1 Assignment Distribute team exercise due 02/05/2024 at 2:30 Enable chapter questions due 02/05/2024 at 2:00

	Examine the impact of AI on privacy.		
Session 3 **02/05/2024**	**Governance and Strategic Planning for Managing Security** • Identify the key organizational stakeholders that are actively involved in planning and their roles. • Discuss strategic organizational planning for information security (InfoSec) • Define the importance, benefits, and outcomes of information security governance	3	Review Team Exercise #2 Assignment Distribute team exercise due 02/12/2024 at 2:30 Enable questions due 02/12/2024 at 2:00
Session 4 **02/12/2024**	**Managing and Creating the Security Policy** • Define information security policy and discuss making them successful. • Describe the major types of information security policy and discuss the major components of each. • Discuss the process of developing, implementing, and maintaining various types of information security policies.	4	Review Team Exercise #3 Assignment Distribute team exercise due 02/26/2024 at 2:30 Enable questions due 02/26/2024 at 2:00
02/19/2024	**HOLIDAY – No class**		
Session 5 **02/26/2024**	**Managing the Security Program through Policy and Experience** • Identify the functional components of an information security program. • Discuss how to plan and staff an organization's information security program.	5	Review Team Exercise #4 Assignment Distribute team exercise due 003/04/2024 at 2:30 Enable questions due 03/04/2024 at 2:00

	• Review the internal and external factors that influence the activities and organization of an information security program. • Discuss the components of a security education, training, and awareness program and explain how organizations create and manage these programs. • Discuss the role of project management in information security.		
Session 6 03/04/2024	**Risk Management and Assessing the Risk** • Define risk management and its role in the organization. • Describe risk management techniques to identify and prioritize risk factors for information assets. • Explain how risk is assessed based on the likelihood of adverse events and the effects on information assets when events occur. • Discuss the use of the results of the risk identification process.	6	Review Team Exercise #5 Assignment Distribute team exercise due 03/11/2024 at 2:30 Enable questions due 03/11/2024 at 2:00
Session 7 03/11/2024	**Using Security to Treat Risk** • Identify the strategy options used to treat risk and be prepared to select from them when given background information. • Evaluate control alternatives under the defense risk treatment strategy and formulate a cost-benefit	7	Review Team Exercise #6 Assignment Distribute team exercise due 03/25/2024 at 2:30 Enable questions due 03/25/2024 at 2:00

	analysis (CBA) using existing conceptual frameworks. • Explain how to maintain and perpetuate controls. • Common approaches used in industry to manage risk. .		
03/18/2024	**SPRING BREAK – No class**		
Session 8 03/25/2024	**Security Management Models** • Describe the dominant InfoSec management models, including national and international standards-based models. • Explain why access control is an essential element of InfoSec management. • Recommend an InfoSec management model and explain how it can be customized to meet the needs of a particular organization. • Describe the fundamental elements of key InfoSec management practices.	8	Review Team Exercise #7 Assignment Distribute team exercise due 04/01/2024 at 2:30 Enable questions due 04/01/2024 at 2:00
Session 9 04/01/2024	**Security Management Practices** • Identify the elements of key information security management practices. • Information security constraints on general hiring processes. • Explain the role of information security in employee terminations. • Describe the security practices used to regulate employee behavior and prevent misuse of information.	9	Review Team Exercise #8 Assignment Distribute team exercise due 04/08/2024 at 2:30 Enable questions due 04/08/2024 at 2:00

	• Discuss the various types of benchmarking and their use in security planning.		
Session 10 **04/08/2024**	**Planning for Contingencies** • Discuss the need for contingency planning. • Describe the major components of incident response, disaster recovery, and business continuity. • Define the components of crisis management and business resumption. • Discuss how the organization would prepare and execute a test of contingency plans.	10	Review Team Exercise #9 Assignment Distribute team exercise due 04/15/2024 at 2:30 Enable questions due 04/15/2024 at 2:00
Session 11 **04/15/2024**	**Maintaining Security** • Discuss the need for ongoing maintenance of the information security program. • Define a model for a maintenance program. • Identify the key factors involved in monitoring the external and internal environment. • Describe how planning, risk assessment, vulnerability assessment, and remediation tie into information security maintenance. • Explain how to build readiness and review procedures into information security maintenance.	11	Review Team Exercise #10 Assignment Distribute team exercise due 04/22/2024 at 2:30 Enable questions due 04/22/2024 at 2:00
Session 12 **04/22/2024**	**Protection Mechanisms**	12	Review Team Exercise #11 Assignment

	• Describe the various access control approaches, including authentication, authorization, and biometric access controls. • List and discuss the various types of firewalls and the common approaches to firewall implementation. • Define and describe the types of intrusion detection and prevention systems and the strategies on which they are based. • Explain the unique challenges associated with physical security and discuss how physical security can supersede computer security. • Explain cryptography and the encryption process and compare and contrast symmetric and asymmetric encryption.		Distribute team exercise due 04/19/2024 at 2:30 Enable questions due 04/29/2024 at 2:00
Session 13 04/29/2024	**Semester Review**	13	Review Team Exercise #12 Assignment Final Paper Deliverable Review
Session 14 05/06/2024	**FINAL Presentations**	14	

NOTES:

The syllabus may be modified to better meet the needs of students and to achieve the learning outcomes.

The School of Professional Studies (SPS) and its faculty celebrate and are committed to inclusion, diversity, belonging, equity, and accessibility (IDBEA), and seek to embody the IDBEA values. The School of Professional Studies (SPS), its faculty, staff, and students are committed to creating a mutually respectful and safe environment (*from the SPS IDBEA Committee*).

NYU SCHOOL OF PROFESSIONAL STUDIES

NYU SCHOOL OF PROFESSIONAL STUDIES

New York University School of Professional Studies Policies

1. Policies - You are responsible for reading, understanding, and complying with University Policies and Guidelines, NYU SPS Policies and Procedures, and Student Affairs and Reporting.

2. Learning/Academic Accommodations - New York University is committed to providing equal educational opportunity and participation for students who disclose their dis/ability to the Moses Center for Student Accessibility. If you are interested in applying for academic accommodations, contact the Moses Center as early as possible in the semester. If you already receive accommodations through the Moses Center, request your accommodation letters through the Moses Center Portal as soon as possible (mosescsa@nyu.edu | 212-998-4980).

3. Health and Wellness - To access the University's extensive health and mental health resources, contact the NYU Wellness Exchange. You can call its private hotline (212-443-9999), available 24 hours a day, seven days a week, to reach out to a professional who can help to address day-to-day challenges as well as other health-related concerns.

4. Student Support Resources - There are a range of resources at SPS and NYU to support your learning and professional growth. For a complete list of resources and services available to SPS students, visit the NYU SPS Office of Student Affairs site.

5. Religious Observance - As a nonsectarian, inclusive institution, NYU policy permits members of any religious group to absent themselves from classes without penalty when required for compliance with their religious obligations. Refer to the University Calendar Policy on Religious Holidays for the complete policy.

6. Academic Integrity and Plagiarism - You are expected to be honest and ethical in all academic work. Moreover, you are expected to demonstrate how what you have learned incorporates an understanding of the research and expertise of scholars and other appropriate experts; and thus recognizing others' published work or teachings—whether that of authors, lecturers, or one's peers—is a required practice in all academic projects.

Plagiarism involves borrowing or using information from other sources without proper and full credit. You are subject to disciplinary actions for the following offenses which include but are not limited to cheating, plagiarism, forgery or unauthorized use of documents, and false form of identification

Turnitin, an originality detection service in NYU Brightspace, may be used in this course to check your work for plagiarism.

Read more about academic integrity policies at the NYU School of Professional Studies on the Academic Policies for NYU SPS Students page.

7. Use of Third-Party Tools - During this class, you may be required to use non-NYU apps/platforms/software as a part of course studies, and thus, will be required to agree to the “Terms of Use” (TOU) associated with such apps/platforms/software.

These services may require you to create an account but you can use a pseudonym (which may not identify you to the public community, but which may still identify you by IP address to the company and companies with whom it shares data).

You should carefully read those terms of use regarding the impact on your privacy rights and intellectual property rights. If you have any questions regarding those terms of use or the impact on the class, you are encouraged to ask the instructor prior to the add/drop deadline.