# Syllabus

This is a single, concatenated file, suitable for printing or saving as a PDF for offline viewing. Please note that some animations or images may not work.

# Course Description

This module is also available as a concatenated page, suitable for printing or saving as a PDF for offline viewing.

**MET CS684**

**IT Security Policies and Procedures**

This course enables IT professionals to implement security policies to support organizational goals. We discuss methodologies for identifying, quantifying, mitigating, and controlling security risks. Students learn to write IT risk management plans, standards, and procedures that identify alternate sites for processing mission-critical applications, and techniques to recover infrastructure, systems, networks, data, and user access.

The course also discusses disaster recovery; handling information security; protection of property, personnel and facilities; protection of sensitive and classified information; privacy issues; and hostile activities.

## Technical Notes

The table of contents expands and contracts (+/- sign) and may conceal some pages. To avoid missing content pages, you are advised to use the next/previous page icons in the top right corner of the learning modules.

This course requires you to access files such as word documents, PDFs, and/or media files. These files may open in your browser or be downloaded as files, depending on the settings of your browser.

# Course Learning Objectives

Upon successful completion of this course you will understand:

- The common Information Systems Security models
- Security characteristics, threats and responses
- Security measures from Technology, Policy and Practice, and Education, Training, and Awareness

dimensions

- Risk management—identification, quantification, response, and control
- Disaster recovery procedures and countermeasures for the business enterprise

# Course Outline

## Module 1: Introduction and Threats to the I.T. Environment

- Threats to enterprise security
- Overview of enterprise I.T. threat responses
- Common enterprise security issues
- Specialized enterprise security issues

## Module 2: Security Policies

- Policies vs. standards vs. procedures
- Policies in detail
- Security policy tiers

## Module 3: Security Standards and Procedures

- Security Standards
- Procedures for security
- Classifying assets

## Module 4: Operational Security Management

- Managing operational security
- Introduction to Business Continuity

## Module 5: Business Continuity and Disaster Recovery

- Continuity and Disaster Recovery
- Preparing for I.T. Continuity
- Managing Disaster Recovery

## Module 6:  Managing Security Risk in System Development and Integration

- Security in system development and integration
- Using Quality to assess security risk in system development

## Module 7: Prepare for and take the final exam

Prepare for and take the proctored final exam.

The course will remain open two weeks after the final exam, so that you can continue discussions and ask any questions about your grades or the course. This is also a time when we enter into a dialog where we endeavor to learn from you how we can modify the course so that it better meets your needs.

# Instructor

**Charles Pak, Ph.D.**

Computer Science
Department
Metropolitan College
Boston University

**Email**: cpak4@bu.edu

Charles Pak earned his Ph.D. in Information Security from Nova Southeastern University, an M.S. in Network Security from Capitol Technology University, and a B.S. in Electrical Engineering from Penn State University. He has taught Information Systems (IS) courses for over 25 years as an IS practitioner and professor. He has managed U.S. Federal Government data centers for over 20 years, including personnel. He has designed, tested, implemented, and maintained many of these enterprise network sites (largest in the world) that encompasses distributed sites across the U.S. as well as the international sites. He has managed state-of-the art systems for military and federal government missions for which he was deployed.

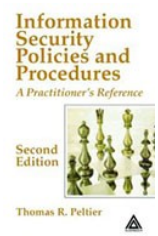
His research topics include Cyber Security, Critical Infrastructure Protection (CIP), PKI, Cyber Counter Terrorism, and Risk Assessment & Management. He has published several research papers in Information Security. As a practitioner, he holds several industry certifications: CISM, CRISC, CISSP, ITIL, SSCP, MCSE, MCT, and CCNA.

Recent Publications:

- Pak, C. (2011). Near Real-time Risk Assessment Using Hidden Markov Models. Nova Southeastern University, ProQuest Dissertations and Theses,ISBN:9781124992945.
- Pak, C. & Cannady, J. (2010). Risk Forecast Using Hidden Markov Models. Research in Information Technology (RIT), ACM, SIGITE, 7(2), 4-15.
- Pak, C. & Cannady, J. (2009). Asset Priority Risk Assessment Using Hidden Markov Models. Proceedings of the 10th ACM SIGITE, Fairfax, Virginia, 2009, 65-73.
- Pak, C. (2008). The near real time statistical asset priority driven (nrtsapd) risk assessment. Proceedings of the 9th ACM SIGITE, Cincinnati, Ohio, 2008, 105-112.

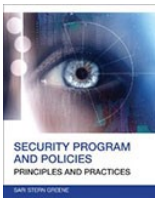
# Course Materials and Resources

## Required Course Books




Peltier, T. R. (2004). *Information security policies and procedures: A practitioner's reference* (2nd ed.). New York, NY/London: Auerbach Publications.
ISBN: 9780849319587

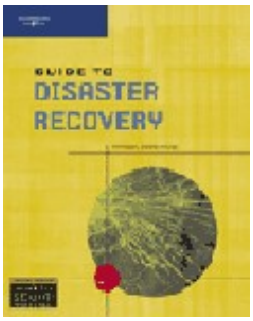
If you use the Peltier ebook, you will find the table of contents (ToC) useful in matching the ebook pages with the hardcover version.




Greene, S. S. (2014). *Security program and policies: Principles and practices* (2nd ed.). (n.p.): Pearson.
ISBN: 9780789751676

These textbooks can be purchased from Barnes and Noble at Boston University.

## Optional Course Book




Erbschloe, M. (2003). *Guide to Disaster Recovery.* Boston: Thomson Course Technology.
ISBN: 9780619131227

This textbook can be purchased from Barnes and Noble at Boston University.

## Boston University Library Information

Boston University has created a set of videos to help orient you to the online resources at your disposal. An introduction to the series is below:

met_ode_library_14_sp1_00_intro video cannot be displayed here

All of the videos in the series are available on the Online Library Resources page, which is also accessible from the Campus Bookmarks section of your Online Campus Dashboard. Please feel free to make use of them.

As Boston University students, you have full access to the BU Library. From any computer, you can gain access to anything at the library that is electronically formatted. To connect to the library, use the link http://www.bu.edu/library. You may use the library's content whether you are connected through your online course or not, by confirming your status as a BU community member using your Kerberos password.

Once in the library system, you can use the links under “Resources” and “Collections” to find databases, eJournals, and eBooks, as well as search the library by subject. Some other useful links follow:

Go to Collections to access eBooks and eJournals directly.

If you have questions about library resources, go to Ask a Librarian to email the library or use the live-chat feature.

To locate course eReserves, go to Reserves.

Please note that you are not to post attachments of the required or other readings in the water cooler or other areas of the course, as it is an infringement on copyright laws and department policy. All students have access to the library system and will need to develop research skills that include how to find articles through library systems and databases.

## Free Tutoring Service

Free online tutoring with SMARTHINKING is available to BU online students for the duration of their courses. The tutors do not rewrite assignments, but instead teach students how to improve their skills in the following areas: writing, math, sciences, business, ESL, and Word/Excel/PowerPoint.

You can log in directly to SMARTHINKING from Online Campus by using the link in the left-hand navigation menu of your course.


YouTube

### Please Note

SMARTHINKING may be used only for current Boston University online courses and career services. Use of this service for purposes other than current coursework or career services may result in deactivation of your SMARTHINKING account.

## Study Guide

### Module 1 Study Guide and Deliverables

**Readings:**

- Greene: Chapter 1, pp. 2–21
- Peltier: pp. 187–188, 250–263, 287–296, and 367–370

**Discussions:** Please complete the Introduction Discussion before you continue in the course.

Discussion 1 postings end Tuesday,

November 6 at 6:00 a.m. ET

**Assignments:** Assignment 1 due Tuesday, November 6 at 6:00 a.m. ET

**Live Classroom:**
- Thursday, November 1 at 7 p.m. ET
- Facilitator live session: TBD

## Module 2 Study Guide and Deliverables

**Readings:** Greene: Chapter 2, pages 32 - 53
Peltier: Primary: pp. 47–80;
Secondary: pp. 199–241

**Discussions:** Discussion 2 postings end Tuesday, November 13 at 6:00 a.m. ET

**Assignments:** Assignment 2 due Tuesday, November 13 at 6:00 a.m. ET

**Live Classroom:**
- Thursday, November 8 at 7 p.m. ET
- Facilitator live session: TBD

## Module 3 Study Guide and Deliverables

**Readings:**
- Greene: Chapter 5, pages 124–144
- Peltier pp. 243–245 and 256–262
- Peltier pp. 85–88 and 95–101

**Discussions:** Discussion 3 postings end Tuesday, November 20 at 6:00 a.m. ET

**Assignments:** Assignment 3 due Tuesday, November 20 at 6:00 a.m. ET

**Live Classroom:**
- Thursday, November 15 at 7 p.m. ET
- Facilitator live session: TBD

## Module 4 Study Guide and Deliverables

**Readings:**
- Greene: Chapter 11, pp. 328–354
- Peltier: pp. 341, 347–348, and 350–358

**Discussions:** Discussion 4 postings end Tuesday, November 27 at 6:00 a.m. ET

**Assignments:** Assignment 4 due Tuesday, November 27 at 6:00 a.m. ET

**Live Classroom:**
- Thursday, November 22 at 7 p.m. ET
- Facilitator live session: TBD

## Module 5 Study Guide and Deliverables

**Readings:** Greene: Chapter 12, pp. 370–397

**Discussions:** Discussion 5 postings end Tuesday, December 4 at 6:00 a.m. ET

**Assignments:** Assignment 5 due Tuesday, December 4 at 6:00 a.m. ET

**Live Classroom:**
- Thursday, November 29 at 7 p.m. ET

- Facilitator live session: TBD

### Module 6 Study Guide and Deliverables

| | |
|---|---|
| **Readings:** | Peltier p. 34 |
| **Discussions:** | Discussion 6 postings end Tuesday, December 11 at 6:00 a.m. ET |
| **Assignments:** | none |
| **Live Classroom:** | • Thursday, December 6 at 7 p.m. ET<br>• Facilitator live session: TBD |

### Final Exam Details

The Final Exam is a proctored exam available from **December 12 at 6:00 a.m. ET to December 15 at 11:59 p.m. ET**. The Computer Science department requires that all final exams be proctored.

**You will receive a technical support hotline number before the start of the exam. Please bring this number with you to the exam.**

# Course Grading Information

## Grading Policy

All students will be expected to demonstrate knowledge of IT Security Policies and Procedures. To obtain an exceptional grade you have to exceed expectations in your assignments, discussions and proctored final exam.

### Grading Structure and Distribution

The grade for the course is determined by the following:

Overall Grading Percentages

| | |
|---|---|
| Assignments | 50% |
| Discussions | 20% |
| Proctored Final Examination | 30% |
| **Total Possible** | **100%** |

The next table shows the minimum points for each letter grade, which is a slightly augmented form of the registrar's system. To get an "B+" for the course, for example, your course points should be at least 3.3. The only exception is that to obtain an A for the course, a score of 3.85 or more is required.

The following grade structure (the university's, with two refinements) will be applied for your assignments:

| Grading Scale | | |
|---|---|---|
| Letter Grade | 100 pt. scale | 4 pt. scale |
| A | 95-100 | 4 |
| A- | 90-94 | 3.7 |
| B+ | 86-89 | 3.3 |
| B | 82-85 | 3 |
| B- | 78-81 | 2.7 |
| C+ | 74-77 | 2.3 |
| C | 70-73 | 2 |
| C- | 67-69 | 1.7 |
| D | 60-66 | 1 |
| F | 0-59 | 0 |

## Assignments

Your homework assignments are an integral part of the learning process. You will receive feedback from your facilitator for each assignment. Please review the assignment rubric.

| | D | C− | C+ | B− | B+ | A |
|---|---|---|---|---|---|---|
| Clarity | Disorganized or hard-to-understand | | Satisfactory but some parts of the submission are disorganized or hard to understand | Generally organized and clear | Very clear, organized and persuasive presentation of ideas and designs | Exceptionally clear, organized and persuasive presentation of ideas and designs |
| Technical Soundness | Little understanding of, or insight into material technically | | Some understanding of material technically | Overall understanding of much material technically | Very good overall understanding of technical material, with some real depth | Excellent, deep understanding of technical material and its inter-relationships |
| Thoroughness & Coverage | Hardly covers any of the major relevant issues | | Covers some of the major relevant issues | Reasonable coverage of the major relevant areas | Thorough coverage of almost all of the major relevant issues | Exceptionally thorough coverage of all major relevant issues |
| Relevance | Mostly unfocused | Focus is off topic or on insubstantial or secondary issues | Only some of the content is meaningful and on topic | Most or all of the content is reasonably meaningful and on-topic | All of the content is reasonably meaningful and on-topic | All of the content is entirely relevant and meaningful |
| Utilization of resources | No useful use of notes, text(s), or Web with incorrect details or applicability | | Some useful use of notes, text(s), or Web with | Fairly good use of notes, text(s), or Web with | Very good use of notes, text(s), or Web with | Excellent use of notes, text(s), or Web with |

| | | | | | |
|---|---|---|---|---|---|
| | | mostly correct details or applicability | correct details or applicability | correct details or applicability | entirely correct details or applicability |

## Discussions

Graded Discussions - you will participate in discussions that will be graded using the A = 4.0, B = 3.0, etc. scale described above. Each week's discussions are to concern only the online notes or the textbook readings. The post subject should be the relevant section: e.g, "5.9 **Real-Life Security Procedures"**

Graded discussion periods are held from Day 1 of each module until 6:00 AM ET on Day 1 of the following module. You are certainly welcome to continue a discussion past the grading period, but that additional posted material will not affect your discussion grade.

| | |
|---|---|
| Relevance | This criterion is designed to keep you focused. It concerns the degree to which your postings are relevant to the week's material. Meaningful questions about material in the notes or the book may qualify also. (This should be an easy way for you to keep your discussion grade in reasonable territory.) |
| Degree of substance | This assesses the management or technical content of your posts, taken as a whole. This is most commonly achieved by putting the content of the notes or books in your own words or by giving examples that you have come across. Meaningful questions about material in the notes or the book may qualify also. Normally, interactive posts with no management or technical content will not count against you here (e.g., we encourage you to let a fellow student know that you found a post interesting or useful). |
| Usefulness of your week's contributions for the rest of your group | This evaluates how useful to your fellow students the totality of your comments and questions are in the context of each week's specified focus. "A" work will result from a significant set of comments and questions that are very useful to you and to the class. This criterion encourages you to be *participatory* (e.g., by responding to good questions or points posed by others). You should have an *even rate* of substantive postings throughout the week. (Contributions posted only at the end of the week are far less useful to your classmates.) If your posts are *long*, they are less likely to be read by others, and this *reduces their usefulness*. This is the only criterion affected by quantity. For example, if you make no posts, they can't be called useful. |

## Class Discussions & Topics for Consideration

Class Discussion options are listed below. Discussions are graded. Your posts are not editable once they have been submitted. It is important for students to start new discussions as well as reply to discussions from other students. For students having difficulty getting started or selecting a relevant discussion topic, several "Additional Discussion Topics for Consideration" are listed below – Option 3, that can be utilized as well.

Discussion options are listed below:

1. Discussions should be focused on the lecture material included in each module. When doing so be sure to reference the Module # and subject topic – (Ex. Module 1: Subject: 2.2 Threat Sources: My interpretation of “Threat”.
2. Current Events: Students can select discussion topics relevant to current events (within the last 12 months). When selecting topics be sure to relate it back to the specific Module #. (Ex. Module 1: Subject *[Cite current event]* – How this event relates to my interpretation of “Threats and Threat Actors related to *[current event] and how this could have been prevented*”.
3. Additional Module Discussion Topics for Consideration (below): For those having difficulty with selecting discussion topics, the following list has been created for your consideration.

## Additional Discussion Topics for Consideration

1. **Defense in Depth**

   Defense in Depth is a widely used and accepted strategy for achieving information Assurance. To review what Defense in Depth is and some background visit any of the following:

   - Defense in Depth
   - Global Information Assurance Certification Paper

   Do you think that Defense in Depth has become irrelevant? How about when we approach service models of IT? Why or why not? What roles do you think policies, standards and procedures play in a defense in depth strategy? What role, of any should Defense in Depth play in SLA evaluations?

2. **Cloud Services**

   With the transition to Cloud services, “leaking cloud buckets” (<-LOL This) is a common term to describe data leaks on public clouds. These can have huge implications. The article points to five steps organizations can take. My questions is the following, what role realignment do you think necessary for successful delivery of these services and controls? You can consider the perspective either from the development team, compliance offices or security officers? Do you think Government is Agile enough to make this happen? Where have they may have failed or succeeded? What are regulated industries doing in terms of realigning the delivery of IT that may meet the high government security requirements?

How Agencies Can Avoid Breaches from Leaking Cloud Storage Buckets

3. **Homeland Security Today.US**

   For relevant and timely Cybersecurity stories, navigate to: Homeland Security Today.US < Subject Matter Areas < Cybersecurity and select one of the articles listed to write about. As with any reference, be sure to properly cite your source.

4. **GDPR**

   GDPR has changed the rules for many organizations. To turn it on its head, read the following article that summarizes how GDPR outlines how cloud providers can attract banking customers. What are some of the ways, technically and organizationally, do you think the customer, in this case a bank using the providers cloud services, should address the partnership? What are some of the security policies/procedures that should be considered or addressed? What would you focus on, organizational issues or technical issues first? How should an organization address multi jurisdiction compliance, all in approach?

   GDPR Gives Cloud Providers Scope to Attract Banks as Customers

5. **Data Privacy & Information Security**

   If we were to look at a Vin Diagram of Data Privacy and Information Security, they would have similarities were the topics overlap and other areas that are not related at all. Describe the differences between the two topics as well as the similarities they share.

6. **Data Privacy within the U.S vs. Data Privacy within the European Union**

   Data privacy is viewed differently throughout the world. There are many differences between the expectations and scope of Data Privacy in the United States vs. those in the European Union.

   - What items are considered ‘Personal Data’ in the U.S. vs. E.U.?
   - Does GDPR change the way U.S. companies need to do business in the E.U.?

7. **Reasons for a company to move to "Cloud" providers vs. doing it themselves**

   Cloud (3rd Party) providers are becoming very popular and more and more businesses are moving to outsourced “Cloud” providers for Software, Infrastructure, Platform, etc. Identify reasons why a company would move to external cloud providers versus keeping these functions inhouse with internal IT resources. Take a risk-based approach to why and when it’s better to select in-house vs. cloud and explain your reasoning.

## Proctored Final Exam

You will be responsible for scheduling your own appointment with an approved proctoring option. Detailed instructions about setting up an appointment will be forthcoming from the proctored exam coordinator.

## Expectations

Many learning activities require sharing your assignments and opinions with your classmates. It is, therefore, very important that you, as well as your classmates, submit your assignments on a timely basis. Due dates will be indicated for each assignment in the Assignments section of the course.

## Delays

If, for any reason, you are unable to meet any assignment deadline, contact your Course Facilitator. All times mentioned in the course (unless otherwise specified) are in Eastern Time. All assignments must be completed and must be turned in by their due dates and due times. Extensions may be granted, though only under mitigating circumstances.

**Boston University** Metropolitan College