

COURSE TITLE BLACKBOARD SITE	MIS 7223 – Enterprise Information Security Spring 2011 – http://my.ltu.edu and select CRN 3892
INSTRUCTOR Contact:	Dr. Kamal Kakish Post your questions under “Ask Dr. Kakish” in the BB Discussion Board Send an email for more timely issues - profkakish@gmail.com Call 404-826-6195 for urgent issues and emergencies
SCHEDULE	January 10, 2010 – April 23, 2010 See http://www.ltu.edu/registrars_office/calendar_final_exam.index.asp for LTU academic calendar information.
LEVEL / HOURS PREREQUISITE	Graduate Degree / 3 semester credit hours Graduate level MIS 6013 Minimum Grade of C-
REQUIRED TEXT (See Blackboard for additional resources)	Michael E. Whitman & Herbert J. Mattord, <u>Principles of Information Security</u> , 3rd edition, 2009 CENGAGE – ISBN: 9781423901778 Available for online purchase through LTU Bookstore at: http://lawrence-tech1.bkstore.com/bkstore/TextbookSelection.do?st=489
ADDITIONAL RESOURCES	LTU Online student resources: http://www.ltu.edu/ltuonline/
TECHNICAL SUPPORT	Technical support for using Blackboard is provided by the Helpdesk. Visit www.ltu.edu/ehelp or 248.204.2330 or helpdesk@ltu.edu

COURSE SCHEDULE FOR COLLEGE OF MANAGEMENT SEMESTER COURSES

This fully online course begins with a partial week online course orientation period to familiarize yourself with the online learning environment and to meet online or via the phone with your instructor. Each subsequent week starts on a Monday and ends on a Sunday. **Assignments are due by 11:59 p.m. EST of Sundays at the end of the week.**

Dates	Modules	Topics / Readings	Assignments Due
Prior to Semester Start and Jan 10 – Jan 12	Module 0	Overview of textbook Online Learning Orientation Course Orientation	Course orientation Instructor conversation Autobiography (BIO): See details under Assignments below View/Submit Assignment Link . (BIO)
Week of Jan 10 – Jan 16	Module 1	Chapter 1 – Introduction to Information Security	Discussion Board Forums (1 st Half) A1. Submit via View/Submit Link . Complete Quiz 1
Week of Jan 17 – Jan 23	Module 2	Chapter 2 – The Need for Security	Discussion Board Forums A2. Submit using View/Submit Link . Chapter Quiz 2
Week of Jan 24 – Jan 30	Module 3	Chapter 3 – Legal, Ethical, and Professional Issues in Information Security	Discussion Board Forums A3. Submit using View/Submit Link . Chapter Quiz 3
Week of Jan 31 – Feb 6	Module 4	Chapter 4 – Risk Management	Discussion Board Forums A4. Submit using View/Submit Link . Chapter Quiz 4
Week of Feb 7 – Feb 13	Module 5	Chapter 5 – Planning for Security	Discussion Board Forums No Assignment. Study for the Midterm Chapter Quiz 5
Week of Feb 14 – Feb 20	Module 6	MIDTERM ESSAY EXAM Chapter 6 – Security Technology: Firewalls & Identifying & Assessing Risk	Discussion Board Forums MIDTERM ESSAY EXAM Submit using View/Submit Assignment Link . Chapter Quiz 6
Week of Feb 21 – Feb 27	Module 7	Chapter 7 – Security Technology: Intrusion Detection, Access Control, & Other Security Tools	Discussion Board Forums A5 Submit using View/Submit Link . Chapter Quiz 7
Week of Feb 28 – Mar 6	Module 8	Chapter 8 – Cryptography	Discussion Board Forums A6. Submit using View/Submit Link Chapter Quiz 8
Mid semester Break – No Classes			
Week of Mar 14 – Mar 20	Module 9	Chapter 9 – Physical Security	Discussion Board Forums (2 nd Half) A7. Submit using View/Submit Link . Chapter Quiz 9
Week of Mar 21 – Mar 27	Module 10	Chapter 10 – Implementing Physical Security	Discussion Board Forums Chapter Quiz 10
Week of Mar 28 – Apr 3	Module 11	Chapter 11 – Security and Personnel	Discussion Board Forums A8. Submit using View/Submit Link . Chapter Quiz 11
Week of Apr 4 –	Module 12	Chapter 12 – Information Security Maintenance	Discussion Board Forums A9. Submit using View/Submit Link

Dates	Modules	Topics / Readings	Assignments Due
Apr 10			Chapter Quiz 12
Week of Apr 11 – Apr 17	Module 13	Final Exam Last chance to turn in any missing work.	Essay Final Exam - Submit using View/Submit Link .

STUDENT EVALUATION

The course has assignments totaling 1000 points. Letter grades are awarded based on the total number of points achieved. **10% per day will be deducted for late assignments and exams.**

	Assignments	Points
P1	Online Discussions (First half)	100
P2	Online Discussions (2 nd half)	100
BIO	Brief Autobiography - BIO	10
A1	A1 - Article	30
A2	A2 - Research	40
A3	A3 - Research	30
A4	A4 - Research	100
A5	A5 - Research	40
A6	A6 - Article	30
A7	A7 - Presentation	50
A8	A8 - Interview	100
A9	A9 - End of Course Report	50
Q1-Q12	12 Chapter Quizzes (Multiple Choice - 10 pts each)	120
M	Midterm Exam - 5 Essay Questions	100
F	Final Exam - 5 Essay Questions	100
	Total Points	1000

Class Points	Letter Grade
95.1 and above	A
90 – 95	A-
87 – 89	B+
83 – 86	B
80 – 82	B-
77 – 79	C+
73 – 76	C
70 – 72	C-
61 – 70	D (Undergrad Only)
60 and below	E

Note: Grades lower than a "B" fall below the LTU graduate standard

Educational Goals

This course is intended to introduce students to Enterprise Information Security from a management perspective. We will first start off by defining Information Security and how important information is as an asset to an organization.

What is the risk of not addressing information security? The proliferation of worms, viruses, and spam continues to grow at an alarming rate and puts an increased strain on IT departments globally. Would you believe it is estimated that anywhere from 50% to 80% of the e-mail on the Internet today is Spam? There have been more worms released in the last 6 months than the previous 10 years. This pace continues. The impact to businesses as security issues continues to grow.

We will look at planning for security. Security is more than just throwing a firewall on your Internet connection and some type of anti-virus software on your PC. You need to protect information, whether it's in the form of Hard Copy, stored on an electronic medium, or during transmission. Each require different methods, and it all starts with planning and establishing security policies.

We will look at risk assessment and how that plays into how much you are willing to spend to protect your information. You would expect a bank to spend more to protect their information than a coffee shop would to express theirs. In fact some industries have established their own standards such as the HIPPA standards for the health care industry.

Finally as we wind down we'll discuss the challenges associated with maintaining Information Security and handling change control to insure that an organization's security objectives are met.

In order to develop a thorough understanding of these areas the instructor employs several teaching methods. Lectures will cover major points from the text and course handouts. Students will learn from the text, from class discussions, individual and group assignments, presentations, and the opportunity to evaluate grasp of the material through a midterm and final exam.

Objectives

- Terms and Concepts - Students will be able to identify:
 - The difference between Information Management and General Management
 - Definition and Characteristics of Information Security and key concepts
 - Differentiate between:
 - Physical Security
 - Personal Security
 - Operational Security
 - Communications Security
 - Security
 - Importance of Policy to guide Information Security Decisions
 - Roles within a security organization
 - What are Worms, Viruses, Trojan Horses, and Spam
 - What are some of the tools used by a Security Organization such as clear communication, and what tools such as ID cards, biometrics, passwords, encryption, firewalls, intrusion detection devices, anti-virus software, updates and patches to existing software, Spam filtering, SSL, IPSec, etc...
 - Law and Ethics
- Business Situation Analysis – Evaluate the impact of information security on businesses today. Evaluate methods of securing information and the price associated with different methods, and what is appropriate to spend to secure information.
- Industry Knowledge - Students will explore current industry trends and developments in Enterprise Information Security through in class article reviews, and an end of term "Information Security Subject Matter" paper and presentation.

Instructional Methods and Course Organization

A variety of instructional methodologies are used in this course. List the specific methods used in your course, which may include but are not limited to:

- **Blackboard learning environment** – Blackboard at my.ltu.edu contains the syllabus, all assignments, reading materials, streaming videos, narrated PowerPoint mini-lectures, podcasts, written lecture notes, chapter quizzes, links to Web resources, and discussion forums. You will submit all assignments via Blackboard, and are expected to participate regularly in discussion topics. Please take time to familiarize yourself with the organization of the Blackboard site. You will want to check the site frequently for announcements reminding you of new resources and upcoming assignments.
- **Student/Instructor Conversations** – Students keep in touch with the instructor via e-mail messages, telephone conference calls, and IM conversations.
- **Self-assessments** – Pre- and post- self-assessment tools will help students measure their entering skills and progress during the course.
- **Required readings** – Textbook chapters should be read according to the schedule outlined in the syllabus. Chapters will be discussed online.
- **Assignments** – List and briefly describe assignments here.

Class Policies and Expectations

I plan to offer you a valuable learning experience, and expect us to work together to achieve this goal. Here are some general expectations regarding this course:

- Each student has a LTU e-mail account. If you wish to use a different e-mail address for this course, please **change your e-mail address in Blackboard under “Student Tools”** and send an e-mail to me so I can store your address in my e-mail directory.
- In a physical sense attendance does not apply directly for this class, but active participation does apply. You are expected to be actively involved in the discussion threads and make two contributory posts a week within the topic for the week. If business travel will take you away from regular participation, please clear these dates with me in advance.
- It is essential that all students actively contribute to the course objectives through their experiences and working knowledge of business and IT.
- All assignments must be submitted on schedule, via Blackboard. If you need to submit an assignment via e-mail, contact the instructor in advance. Late work will be reduced by 10% per day.
- Assignments must be completed to an adequate standard to obtain a passing grade. Requirements for each assignment are detailed in this syllabus and on the LTU Online web site.
- Be prepared to log into Blackboard **at least once each day**. Please focus your on-line correspondence within the appropriate Blackboard discussion forums so that your colleagues can learn from you.
- At the end of the course, you will be invited to participate in a University evaluation of this course. Your feedback is important to the University, to LTU Online, and to me as an instructor, and I encourage you to participate in the evaluation process.
- Honesty - Students are expected to do their own work at all times. While it is acceptable to discuss homework and case assignments with others, students should first attempt to solve assigned work themselves. In no case will copied work from another person be considered acceptable. Any cheating on exams is grounds for failure and will be referred to the Dean for the strongest possible punishment. Plagiarism is also unacceptable; please site all references accordingly in any work that you turn in.
- Conduct - Students are expected to conduct themselves in a professional manner at all times and to be courteous to their classmates.

Homework

In completing homework assignments, instructors expect that students will attempt to solve assigned problems by themselves, or, only if permitted by the instructor, by a group of students. Normally,

instructors allow for general discussion between students about how to solve a problem. In no case, however, is it acceptable for one student to copy a solution from a peer.

Technical Assignments

Technical assignments (such as computer programs) are to be developed by a student's (or team of students if permitted by the instructor) independent effort. As with homework, general discussion between students on how to approach a problem may be acceptable. It is unacceptable, however, to copy a peer's program and submit it as one's own work.

Term Papers and Research Papers

Students may be assigned term papers in their LTU coursework. In grading such papers it is important for instructors to know which ideas are the student's own thoughts and which are either copied or paraphrased from another source. Hence, students must cite their sources using a standard style guide, such as American Psychological Association (APA), or Modern Language Association (MLA), Chicago.

Blackboard Learning Environment – Blackboard at my.ltu.edu contains the syllabus, all assignments, reading materials, streaming videos, narrated PowerPoint mini-lectures, podcasts, written lecture notes, chapter quizzes, links to Web resources, and discussion forums. You will submit all assignments via Blackboard, and are expected to participate regularly in discussion topics. Please take time to familiarize yourself with the organization of the Blackboard site. You will want to check the site frequently for announcements reminding you of new resources and upcoming assignments.

Student/Instructor Conversations – Students keep in touch with the instructor via e-mail messages, telephone conference calls, and IM conversations.

Self-Assessments – Pre- and post- self-assessment tools will help students measure their entering skills and progress during the course.

Required Reading – Textbook chapters should be read according to the schedule outlined in the syllabus. Chapters will be discussed online.

Publisher Web Site – A publisher web site at <http://www.nnn.com/nnn> includes instructional materials, PowerPoint slides, case studies, application exercises, and practice quizzes. You should make use of as many of these resources as you need to be successful.

Assignments – List and briefly describe assignments here.

CLASS POLICIES AND EXPECTATIONS

I plan to offer you a valuable learning experience, and expect us to work together to achieve this goal. Here are some general expectations regarding this course:

Each student has a LTU email account. If you wish to use a different email address for this course, please **change your email address in Blackboard under “Blackboard Tools”, then “Personal Information”** and send an email to me so I can store your address in my email directory.

Readings, discussion forum participation, and written assignments must be completed according to the class schedule. It is important to contact the instructor as needed to discuss personal needs regarding course requirements and assignments.

It is essential that all students actively contribute to the course objectives through their experiences and working knowledge.

All assignments must be submitted on schedule, via Blackboard, and using Microsoft Office compatible software. If you need to submit an assignment via email, contact the instructor in advance.

Assignments must be completed to an adequate standard to obtain a passing grade. Requirements for each assignment are detailed in this syllabus.

Be prepared to log into Blackboard at least once each day. Please focus your online correspondence within the appropriate Blackboard discussion forums so that your colleagues can learn from you.

At midterm and at the end of the course, you will be invited to participate in a University evaluation of this course. Your feedback is important to the University, to LTU Online, and to me as an instructor, and I encourage you to participate in the evaluation process.

It is important for you as students to know what to expect from me as your instructor:

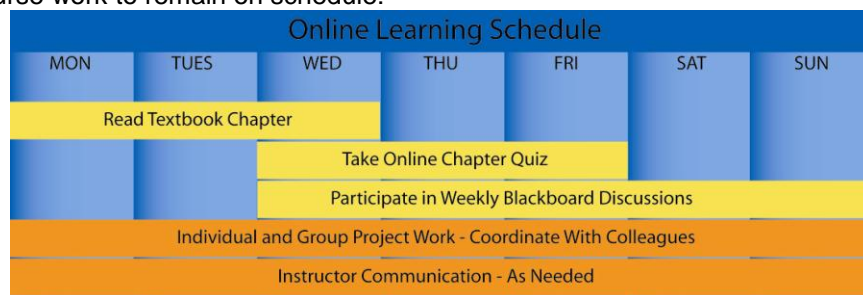
- I will be available to you via e-mail and phone, and will promptly reply to your messages.
- I will be available to you for telephone appointments as requested.
- I will maintain the Blackboard web site with current materials, and will resolve any content-related problems promptly as they are reported to me.
- I will send out frequent e-mail updates to all class members to guide upcoming work and remind you of assignment due dates.
- I will return all assignments to you promptly (usually within 72 hours), and will include individualized comments and suggestions with each assignment.
- I will hold our personal written or verbal communications in confidence. I will not post any of your assignments for viewing by the class without requesting your approval in advance.
- I will treat all members of the class fairly, and will do my best to accommodate individual learning styles and special needs.
- If any of these points need clarification, or when special circumstances arise that require my assistance, please contact me so that we can discuss the matter personally.

PRACTICAL GUIDELINES FOR CLASS LOAD EXPECTATIONS

A three-credit course generally requires at least nine hours per week of time commitment. Here are some practical guidelines to help schedule your time commitments for this online course:

- A 14-week semester would require at least 126 hours of time commitment to successfully complete all readings, activities, assignments, and texts as described in this syllabus.
- You should reserve at least 6 hours per week to read the required textbook chapters and resources, participate in online discussions, review presentation materials, and work through online quizzes. This effort will total at least 84 hours over the course of the semester.
- You should organize your remaining time to roughly correspond with the point value of each major assignment. This means that you should plan to spend at least:
 - 8-9 hours preparing your case study review;
 - 24-40 hours working with your group on the three parts of your semester-long project;
 - 8-9 hours working on the various components of your reflective consolidation (final exam).

These guidelines may not reflect the actual amount of outside time that you – as a unique individual with your own learning style – will need to complete the course requirements. The number of hours each week will vary based on assignment due dates, so please plan ahead to insure that you schedule your academic, work, and personal time effectively. The following graphic can be used to guide you in planning your weekly course work to remain on schedule:



ASSIGNMENT DETAILS

Course assignments and evaluation criteria are detailed below. Please review these requirements carefully. See the section Academic Resources / Assessment Guidelines for information about assessment of written and oral presentations.

Details for all assignments are shown below. Please note that you **should not submit any assignments to the Blackboard “Digital Drop Box” as it is no longer available in BlackBoard**. All assignments are submitted using the **Blackboard “Assignments” or “SafeAssign” function**. Some assignments are also posted to the Blackboard Discussion Forum for student comments.

Assignments and Points

BIO – Autobiography:

For Module 0 - Orientation

Write 1-2 paragraphs on your background & what you want to gain out of this class. Include academic, personal, and professional background as related to this course. Confirm that you have read and will honor LTU's Honor Code. No points awarded without acknowledgement that you have read and will abide by LTU's Honor Code. Submit using the appropriate link in order to get a grade. **Do NOT use the Digital Drop Box.**

A1 – Article:

For Module 1 – Introduction to Information Security

Please find an article that relates to information security and write a summary that is effectively one page long. Please post that summary with either a link or scanned copy of your article. Please also read the articles and summaries posted by your fellow students and provide feedback on your thoughts.

In addition to your Grade Book submission, please create a new thread for your article in the Discussion Board Under “Module 1 Discussion” so that your classmates could benefit from reviewing your research.

P.S. Please RUN your assignment first through SAFEASSIGN BEFORE you submit it. You must get a matching score of <20% to submit for grading. Any matching score over 20% will incur significant deductions. Please learn how to EXCLUDE your References from counting toward your match score.

A2 – Research:

For Module 2 - The need for Security.

Find examples of security breaches (research external to the book) and how they have impacted Enterprise Organizations. This can be anything from the impact of lost/stolen data, to the impact of an attack from a hacker, or an unintentional impact from an internal employee. The objective here is to back up the need for security.

Submit your document with your name and the assignment # (ex: KakishA2.doc) using this View/Submit Assignment link. It should be the equivalent of 3 pages double spaced. Therefore at least 3 examples would be appropriate, and more is better.

P.S. Please RUN your assignment first through SAFEASSIGN BEFORE you submit it. You must get a matching score of <20% to submit for grading. Any matching score over 20% will incur significant deductions. Please learn how to EXCLUDE your References from counting toward your match score.

A3 – Research:

For Module 3 – Legal, Ethical, and Professional Issues in Information Security

Chapter 3 is titled "Legal, Ethical, and Professional Issues in Information Security". There was a ruling recently handed in a case involving TJX the parent company for TJX.

Please answer the following questions for this assignment:

1. What information was stolen from TJX?
2. How was it stolen?
3. What was the penalty handed down?
4. Do you think the penalty was appropriate, and will it act as a deterrent to other hackers?
5. Do you believe TJX had sufficiently protected their customer's data?
6. When such information is stolen, do you believe that the company that lost this information (or had it stolen) should have to make their customers aware that the information was stolen?
7. Also, what would you do if you were in a position of management and such an incident occurred, would you tell your customers? If so, what would you tell them?

Please submit your assignment using the View/Submit Assignment. It should be the equivalent of 3 pages single spaced.

P.S. Please RUN your assignment first through SAFEASSIGN BEFORE you submit it. You must get a matching score of <20% to submit for grading. Any matching score over 20% will incur significant deductions. Please learn how to EXCLUDE your References from counting toward your match score.

A4 – Research

For Module 4 but not for any specific chapter or topic

Security Certification and USA Readiness Research

“Some certifications are hot, some not”.

Security Certification has increasingly become an important consideration among business managers and technical professionals alike. With the advent of 9/11 terrorism and the progressive threats and attacks on computer and data systems worldwide, governments and businesses have sharply increased their requirements for information security certified professionals.

Students should research information on the various types and classifications of Security Certifications from a variety of sources. At minimum students should contrast, compare, and report on the following certifications:

1. CISSP (from ISC2)
2. CompTIA Security+
3. SSCP
4. CISM
5. CCSP
6. Other relevant Certifications and Exams
7. Your personal observations and conclusions on certification

When compiling your Certification Report please be very thorough with the details for each certification. There is no limit to the number of pages for this assignment.

Include information such as the purpose of the certification, who should take it, Body of Knowledge domains, exam requirements, exam prices, exam scores, vendor dependency (proprietary or not), requirements to maintain the certification, pros and cons, and other information relative to the specific certification.

The Certification portion of the assignment is worth 50 points.

In addition, students should visit the Center for National Security Studies (CNSS), US-CERT <http://www.us-cert.gov/>, and other cyber-terrorism and counter-terrorism websites including the Whitehouse and the Department of Homeland Security (DHS), and summarize their findings, assessments, latest developments, and personal opinions regarding the US readiness in combating information threats and attacks, and the degree to which Information Technology is able to address national and global information security issues.

Again, there is no limit to the length of the Readiness Report

The Readiness portion of the assignment is worth 50 points.

P.S. Please RUN your assignment first through SAFEASSIGN BEFORE you submit it. You must get a matching score of <20% to submit for grading. Any matching score over 20% will incur significant deductions. Please learn how to EXCLUDE your References from counting toward your match score.

A5 – Research:

For Module 7 – Security Technology: Intrusion Detection, Access Control, & Other Security Tools + Cryptography

As a subject matter expert, select one of the security technologies or tools you're interested in (ex: IDS, IPS, Firewalls, Cryptography, etc), do a little research, then write a 5-page paper (20 points) APA style, and put together a PowerPoint presentation (10 points). You don't need to actually present the topic, just submit the ppt.

A6 – Article:

For Module 8 – Cryptography

Select a Cryptography article from a reputable institution (ex: IEEE or similar caliber) and summarize it within 3 to 5 pages APA Style, single space, using references within the body of the document and a bibliography section at the end of your document. Make sure you include brief lists of acronyms and glossary for any technical terms.

You are free to include any major topics within this broad subject, but I would like you to consider briefly talking about some or most of the following:

1. The purpose of cryptography
2. Types of cryptographic algorithms: Secret key cryptography, Public-key cryptography, Hash functions, Why three encryption techniques? The significance of key length
3. Trust models: PGP web of trust, Kerberos, Public key certificates and certification authorities
4. Cryptographic algorithms: Password protection, Some of the details of diffie-hellman key exchange, Some of the details of rsa public-key cryptography, Some of the details of DES, breaking DES, and DESvariants

- eLearning Services
5. Protocols: Pretty good privacy (PGP), IP security (ipsec) protocol, The SSL "family" of secure transaction protocols for the world wide web, Elliptic curve cryptography, The advanced encryption standard and rijndael, and Cisco's stream cipher
 6. Your own conclusions and lessons learned, and of course
 7. References and further reading

So, I hope you'll enjoy this exercise, but please don't make it overkill. If you feel that you need to exceed 5 pages, feel free to do so, but don't go overboard. Most importantly, I trust that this report will be your OWN product, not a copy and past quick activity.

P.S. Please RUN your assignment first through SAFEASSIGN BEFORE you submit it. You must get a matching score of <20% to submit for grading. Any matching score over 20% will incur significant deductions. Please learn how to EXCLUDE your References from counting toward your match score.

A7 – Presentation:

For Module 9 – Physical Security

For this last assignment of the course, you need to prepare a **presentation ONLY**. I've waived the requirement of writing a paper.

You may choose any Enterprise Security Topic that relates to Physical Security (ex: Infrastructures, Networks, Data Centers, Surveillance Devices, servers, desktops, laptops, routers, etc)

Your presentation should be between 15 and 20 slides. Anything outside this range will cause point deduction.

A8 – Interview:

For Modules 10 and 11 – Implementing Physical Security **AND** Security and Personnel

Interview an IT Security Manager, an information security officer, or anyone with supervisory responsibilities within a Security Organization

Information Security Manager Interview Paper Guidance

I'm trying to leave some room for interpretation to best allow the students flexibility based on the person they interview. My objective is to give each student the opportunity to learn the business side of what Information Security managers do on a day-to-day basis and how they make their decisions. The paper should be 7 to 12 pages long, single space, and **must include all of the following**:

1. A brief overview of the company
2. A brief overview of the person's background
3. A brief overview of that person's Education
4. Technical background vs. Financial/Business Background
5. What does this individual do on a day to day basis
6. Discussion on how they make decisions: Technical vs. Financial (Price and Budget) vs. Political/Relationships
7. Summary/Conclusion on what you learned

Potential questions you could use during your interview with the selected individual to help drive for the information listed above:

- Describe what you do on a day-to-day basis?
- What would you use as a job description for your current role?
- What type of background would you recommend for your job?
- What things in your background best prepared you for this job?
- What influences your decision more, the technical solution or the price?
- How much does corporate policy do to give you flexibility for your decisions?
- At times does corporate policy dictate your decision and limit your flexibility?
- Discuss a project that you have been involved with that you are the most proud of and why?
- Are there any lessons that you learned the hard way that you could provide some insight into?
- What Security issues worry you the most?
- How has managing information security changed over the last 5 years?
- What do you think will be the greatest security risks over the next 5 years?
- Anything else you'd like to ask

A9 – End of Course Report:

For Module 12

Please summarize what you learned in this course. Write a 5 – 8 page report highlighting the main topics you learned, what you liked best/least and why, and any recommendations you may have for future students.

Quizzes (120 points) Online Discussions (200 Points)

There are 12 quizzes, one per week, for modules 1 through 12.

Each quiz is 20 questions long and worth 10 points.

All quizzes are multiple choice, and are created directly from your textbook.

You may use your textbook in answering the quizzes, but there's a one hour limit for each quiz.

Each student is expected to actively participate in online activities. Class discussions is evaluated to a maximum of 200 points (100 points for each half of the course) according to the criteria discuss in detail in the Discussion Board, but here's a quick synopsis:

Please read these guidelines carefully and follow the instructions accordingly.

Please review the information below for better understanding of your role in on-line participation.

To summarize, you may follow these simple rules:

1. Answer all questions posted by the professor
2. **Participate at least THREE different DAYS each week**
3. Discuss or comment on at least TWO other students' answers/comments.

Your Online Weekly Discussions accounts for a significant portion of your final grade. Therefore, it is very important to understand the discussion grading criteria and requirements.

SYLLABUS ADDENDA

Please see the LTU Online "Current Students" web site <http://www.ltu.edu/ltuonline/> for comprehensive information about Lawrence Tech's academic services, library services, student services, and academic integrity standards. The content of this web site is explicitly included as syllabus requirements.