The Villanova University
Master of Science in Cybersecurity
Department of Electrical and Computer Engineering
ECE 8488
Security Risk Assessment and Management
May 29 - July 29, Summer 2013

Instructor:
Dr. Charles Pak
Email: charles.pak@villanova.edu; charlespak@verizon.net
Email is the best way to contact me. Here is my cell number if needed: (443)610-7986

General Course Information:

This is a graduate level class. Students are expected to apply time management skills to their work, home, and academic life. Any due dates for materials for these classes are designed to spread the workload over the semester. Material, such as reading assignments, with no due date given should be done as soon as possible by the student so the workload does not become overwhelming prior to the end of course.

Course Description

This course presents an overview of the various methodologies that may be used in assessing and managing security risk to achieve information protection in contemporary highly networked enterprises. This class will explore both technology and management issues related to Computer Security Risk Assessment and Management to protect information assets. Specific technologies and techniques used by security managers to protect sensitive, private information are discussed and explored. Countermeasures and safeguards to mitigate risks will be discussed in defense-in-depth. Discussed topics include Network Security Risk Assessment and Management, Threats to Network Security; Techniques and Technologies for Security Management, Managing System Protection; Cryptography; Wireless Security, Disaster Recovery; Legal and Ethical Issues.

Students are reminded that it is a violation of Federal and some states' laws to attempt to gain unauthorized access to information assets or systems belonging to others, or to exceed authorized on systems to which they have been granted access. At no time in this class should any student violate either laws or confidences. Any violation of legal boundaries in the course of this class will be considered a violation of the class trust and will be subject to sanctions in grading.

Course Objectives

Upon completion of this course, the student will be able to:

- Conduct Risk Assessment and Management
- Analyze different risk assessment types
- Describe the essential Computer Security Fundamentals
- Identify and Analyze threats to Network Security
- Describe different Techniques and Technology for Security Management
- Mitigate identified risks
- Monitor and Manage System Protection
- Manage identified risks for organizations

Required Reading Materials:

Books:

Landoll, D. (2011). "The Security Risk Assessment Handbook".
ISBN: 978-1-4398-2148-0, CRC Press

Other Reading Materials:

- Geer, Dan, Jr. "Cybersecurity and National Policy." *Harvard National Security Journal*, Volume 2, Issue 1. Cambridge: MA. January 2010. Available at http://harvardnsj.com/2011/01/cybersecurity-and-national-policy/
- Geer, Dan, Jr., et al. "CyberInsecurity: The Cost of Monopoly." Washington, DC. Computer & Communications Industry Association (CCIA), September 2003. Available at http://cryptome.org/cyberinsecurity.htm
- McGraw, Gary; Chess, Brian; and Migues, Sammy, "Building Security in Maturity Model 2 (BSIMM v2)." May, 2010. Available at http://bsimm.com/download/
- Anderson, Ross. "Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition." Indianapolis: Wiley Publishing, 2008. ISBN: 978-0-470-06852-6. Select Chapters: 11: Physical Protection. Available at http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c11.pdf
- Anderson, Ross. "Security Engineering: A Guide to Building Dependable Distributed Systems." New York: Wiley Publishing, 2001. ISBN-10: 0471389226 / ISBN-13: 978-0471389224. Select Chapters: 18: Network Attack and Defense. Available at http://www.cl.cam.ac.uk/~rja14/Papers/SE-18.pdf Chapters: 22: Management Issues. Available at http://www.cl.cam.ac.uk/~rja14/Papers/SE-22.pdf
- Common Criteria 2.1 download from http://www.niap-ccevs.org/cc-scheme/

Method of Instruction

The method of instruction will combine the following elements:
- Online Discussion
- Risk Assessment Reports
- Risk Assessment Research Paper

Policy on Paper Submission

Papers are due on the date they are due. Up until midnight of that night, no penalty will accrue. Please note that life emergencies happen. Do NOT wait until the last moment to start on your paper. If you do that and something comes up to impede your progress, it will hamper your ability to turn in your paper on time. Papers MUST be submitted electronically via Blackboard.

All papers must include the following statement:
"This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources that I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.

Signature _____"

Reading Assignments:

The scope of this course is very broad, and a large amount of reading is required. However, the relative importance of materials, as specified in the course outline, varies. Specifically assigned materials must be read in detail. Materials to which students are directed or for which copies are provided but which are not specifically assigned are recommended for added understanding of required material, but are optional in the sense that students will not be held explicitly responsible for anything that appears only in these materials. They are appropriate either for students who have difficulty with the subject matter based on the required readings or for those who want a deeper understanding of the material. Recommended background reading is valuable for overall understanding, may provide a technical depth beyond the requirements of the class, may provide valuable material for student research topics, and may be useful in responding to comprehensive essay questions.

Since much of what is happening in information security is happening now, current events will play a role in class discussions. As professionals, it is crucial for you to keep up with events as they unfold. There is no substitute for regular reading of business and technology news in a major newspaper, for following current journal articles, visiting key web sites, and for noting the direction of industry organizations such as the IEEE, IETF, and the ACM. You should constantly consider how what you read in such sources fits into the subject you are studying. Current articles, including Web articles, may be assigned as supplementary reading as the course progresses.

Students are encouraged to use as many and varied sources as possible in exploring the questions presented during the course, and to share those sources with their classmates. References to sources should be explicit in exchanges among the students and instructor, and will be considered in determining the extent to which each student participated for purposes of awarding grades.

Grading Policy:

The overall course grade will be established as follows:

Grading Criteria	Percentage
Discussion Participation	20
Risk Assessment Research Paper	30
Qualitative Risk Assessment Paper	25
Quantitative Risk Assessment Paper	25
Total	**100**

http://www1.villanova.edu/villanova/enroll/registrar/policies.html#question_faq_5

Letter Grade	Approximate percentage grade range	Grade Points
A	95–100	4.00
A−	90 < 95	3.67
B+	85 < 90	3.33
B	80 < 85	3.00
B−	75 < 80	2.67
C+	70 < 75	2.33
C	65 < 70	2.00
F	< 65	0.00

Other Items of Importance

Don’t ask for an incomplete for convenience. The University has very specific policy on when a grade of incomplete may be awarded. See the Bulletin for more information on grading policies.

Writing and Speaking Standards:

Written communication is an important element of the total communication process. This is a graduate program. **Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.** The University recognizes and expects exemplary writing to be the norm for course work. To this end, all papers, individual and group, must demonstrate graduate level writing and comply with and conform to standard academic format as specified in A Manual For Writers of Term Papers, Theses, and Dissertations by Kate L. Turabian, Seventh Edition. Points will be subtracted for format errors. Points will also be subtracted for spelling and grammatical errors. Use of Standard English ensures that your points will be both understood and correctly interpreted by all readers, a skill that will be vital to your success after graduation.

Effective managers, leaders, and teachers are also effective communicators. It is no understatement to say that effective speaking and writing skills are as important to career success as technical mastery of a subject. Speaking and writing effectively are a critical part of this course. Correct and graduate level Standard English must be used.

***Academic integrity*:**
Academic integrity is central to the learning and teaching process. Students are expected to conduct themselves in a manner that will contribute to the maintenance of academic integrity by making all reasonable efforts to prevent the occurrence of academic dishonesty. Academic dishonesty includes, but is not limited to, obtaining or giving aid on an examination, having unauthorized prior knowledge of an examination, doing work for another student, and plagiarism of all types.

Plagiarism is the intentional or unintentional presentation of another person's idea or product as one's own. Plagiarism includes, but is not limited to, the following: copying verbatim all or part of another's written work; using phrases, charts, figures, illustrations, or mathematical or scientific solutions without citing the source; paraphrasing ideas, conclusions, or research without citing the source; and using all or part of a literary plot, poem, film, musical score, or other artistic product without attributing the work to its creator. Students can avoid unintentional plagiarism by following carefully accepted scholarly practices. Notes taken for papers and research projects should accurately record sources of material to be cited, quoted, paraphrased, or summarized, and papers should acknowledge these sources.

There is no such thing as "boilerplate" in academia.

If you don't understand what plagiarism is and how to avoid it, consult the University's academic integrity policy. See also http://www.prism-magazine.org/december/html/student_plagiarism_in_an_onlin.htm
This is a graduate program. Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.

The penalties for plagiarism include a zero or a grade of "F" on the work in question, a grade of "F" in the course, suspension with a file letter, suspension with a transcript notation, or expulsion. Students are not permitted to submit an assignment or paper that already has been submitted for another course at any institution, even if it is entirely their own work. This includes cutting and pasting portions of previous papers or other written assignments. The penalties will be the same as those listed above for plagiarism. Please check your work carefully. Turabian contains complete guidance on how to correctly reference all forms of material.

There is no such thing as "boilerplate" or "standard language" in academia. Students are expected to write their reports themselves. If it is necessary to use material from other sources, it is expected (and mandatory) that the standards of academic style and integrity will be followed. Every student is encouraged to visit these websites for interesting information regarding this issue:

- A true story about plagiarism gone awry
http://www.aweekofkindness.com/blog/archives/the_laura_k_krishna_saga/000023.html (May only be available in a Google Cache as Domain expired 2/23/2011).
- Goucher College's "Plagiarism-by-Paraphrase Risk Quiz"
http://faculty.goucher.edu/writingprogram/sgarrett/Default.html
- Copyright law, frequently asked questions, and other good stuff
http://www.copyright.gov/
- The Islam Online.net Fatwa on Plagiarism
http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503549102

Disabled Students: Any student who has a disability and is in need of special consideration must inform the instructor of this need within the first week of class (or immediately if the disability appears after the first week of class) so that appropriate arrangements can be made. This includes students with reading or learning disabilities who may require extra time on tests. In all cases, the student must communicate with the Disability Services Center and have registered the disability with the University.

Discussion Rubric

Criteria	Non-compliant	Minimal	Compliant	Advanced
One initial major response (minimum 125 words) to first discussion question	Did not complete this portion of the assignment or most of the discussion points were inappropriate or were not identified. (1)	The discussion points were identified and described but with fair accuracy and some of the discussion points were inappropriate or were not identified. (3)	The discussion points were identified and described with good accuracy and appropriate information was identified and discussed. (6)	The discussion points were identified and described with high accuracy and all appropriate information was identified and discussed clearly. (10)
Writing – grammar, sentence structure, paragraph structure, spelling, punctuation (APA required).	5 or more different errors in sentence structure, paragraph structure, spelling, punctuation, or APA usage. References are expected. (Major issues) (1)	3-4 different errors in sentence structure, paragraph structure, or APA usage. References are expected. (Many issues) (3)	1-2 different errors in sentence structure, paragraph structure, spelling, punctuation, or APA usage. References are expected. (Minor issues) (6)	No errors in sentence structure, paragraph structure, spelling, punctuation or APA usage. References are expected. (Minor issues) (10)
Responding to other students.	Did not respond to other students or responses were trite with no substance. (1)	Responded to other students but responses were trite with no substance. (3)	Responded to one other student, response was substantive. (6)	Responded to two or more other students, responses were substantive. (10)
Frequency of responses.	Did not post in the threaded discussion. (1)	Posted one message only 1 day of the week. (3)	Posted more than 1 message but only one day of the week. (6)	Posted on two or more different days of the week. (10)

Course Schedule

Week	Date	Discussion Topic	Assignments Due
1	5/29	Chapter 1 – Introduction to Risk Assessment & Management	Discussion Participation
2	6/5	Chapter 2 – Information Security Risk Assessment Basics Chapter 3 – Project Definition	Discussion Participation
3	6/12	Chapter 4 – Security Risk Assessment Preparation Chapter 5 – Data Gathering	Discussion Participation
4	6/19	Chapter 6 – Administration Data Gathering Chapter 7 – Technical Data Gathering	Discussion Participation
5	6/26	Chapter 8 – Physical Data Gathering Chapter 9 – Security Risk Analysis	Qualitative Risk Assessment Report Discussion Participation
6	7/3	Chapter 10 – Security Risk Mitigation	Discussion Participation
7	7/10	Chapter 11 – Security Risk Assessment Reporting Chapter 12 – Security Risk Project Management	Discussion Participation

8	7/17	Chapter 13 – Security Risk Assessment Approaches	Quantitative Risk Assessment Report Discussion Participation
9	7/24	Final Week – Risk Assessment Research Paper	Risk Assessment Research Paper Discussion Participation

Risk Assessment Project

GLOBAL FINANCE, INC. (GFI)

Global Finance, Inc. (GFI) is a financial company that manages thousands of accounts across Canada, the United States, and Mexico. A public company traded on the NYSE, GFI specializes in financial management, loan application approval, wholesale loan processing, and investment of money management for their customers.

GFI employs over 1,600 employees and has been experiencing consistent growth keeping pace with S&P averages (approximately 8%) for nearly six years. A well-honed management strategy built on scaling operational performance through automation and technological innovation has propelled the company into the big leagues; GFI was only recently profiled in Fortune Magazine.

The executive management team of GFI:

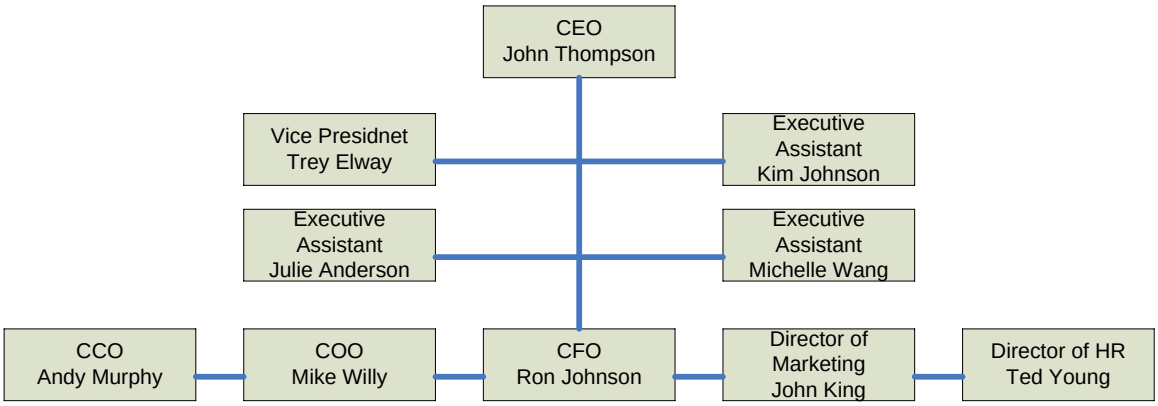


Figure 1 GFI Management Organizational Chart

BACKGROUND AND YOUR ROLE

You are the Computer Security Manager educated, trained, and hired to protect the physical and operational security of GFI's corporate information system.

You were hired by COO Mike Willy and currently report to the COO. You are responsible for a $5.25m annual budget, a staff of 11, and a sprawling and expansive data center located on the 5th floor of the corporate tower. This position is the pinnacle of your career – you are counting on your performance here to pave the way into a more strategic leadership position in IT, filling a vacancy that you feel is so significantly lacking from the executive team.

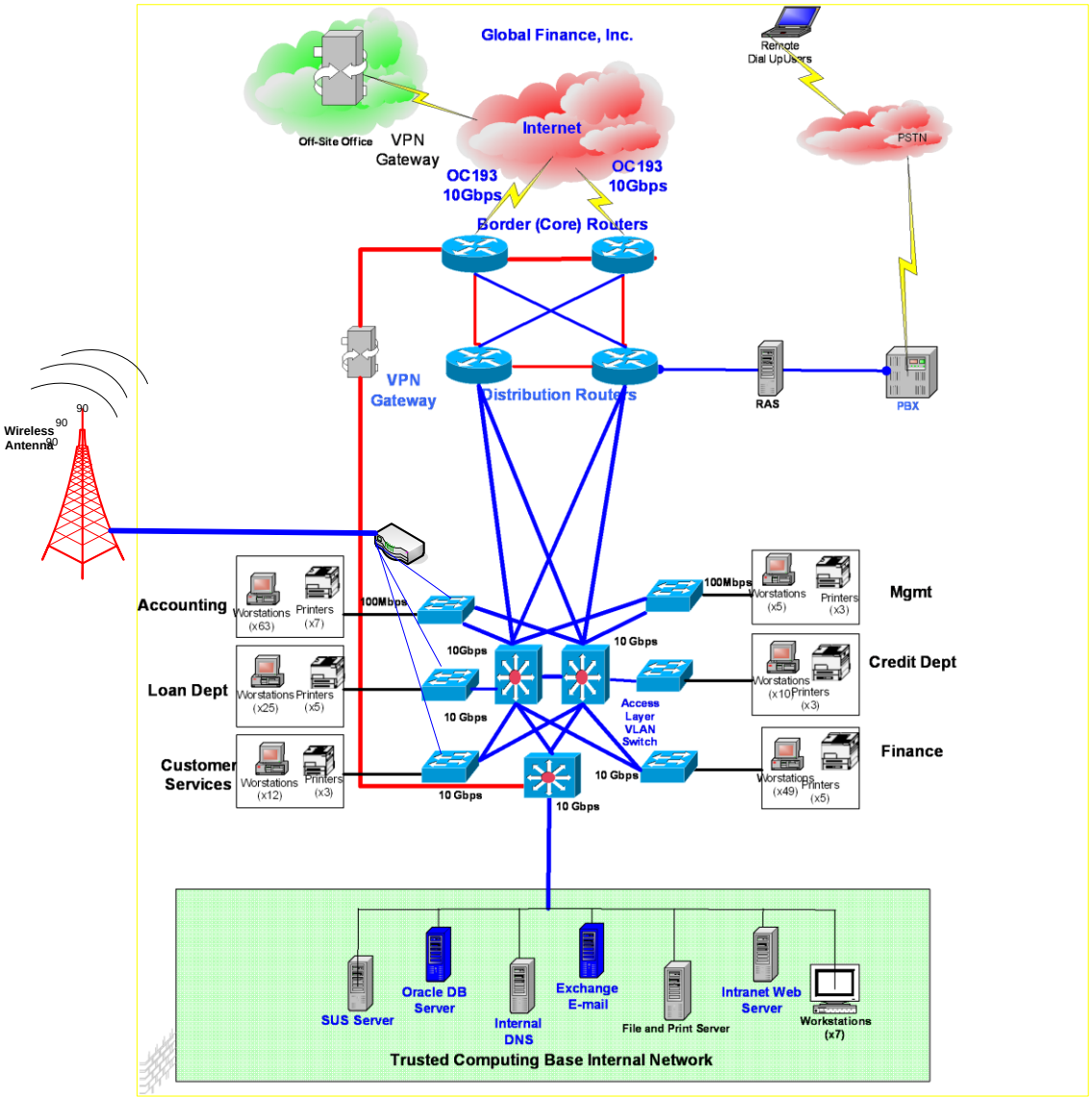
There is actually a reason for this. CEO John Thompson believes that the IT problem is a known quantity – that is, she feels the IT function can be nearly entirely outsourced at fractions of the cost associated with creating and maintaining an established internal IT department; the CEO's strategy has been to prevent IT from becoming a core competency since so many services can be obtained from 3rd parties. Since the CEO

has taken the reigns two years ago, the CEO has made significant headway in cutting your department's budget by 30% and reducing half of your staff through outsourcing. This has been a political fight for you: maintaining and reinforcing the relevance of an internal IT department is a constant struggle. COO Willy's act of hiring you was, in fact, an act of desperation: the increasing operational dependence on technology combined with a diminishing IT footprint gravely concerned Jacobson, and he begged to at least bring in a manager to whom these obligations could be delegated to. Jacobson's worst nightmare is a situation where the Confidentiality, Integrity, and Availability of the information system was compromised – bringing the company to its knees – then having to rely on vendors to pull him out of the mess.

GFI has experienced several cyber-attacks from outsiders over the past a few years. In 2012, the Oracle database server was attacked and its customer database lost its confidentiality, integrity, and availability for several days. Although the company restored the Oracle database server back online, its lost confidentiality damaged the company reputations. GFI ended up paying its customers a large sum of settlement for their loss of data confidentiality. Another security attack was carried out by a malicious virus that infected the entire network for several days. While infected the Oracle and e-mail servers had to be shut down to quarantine these servers. In the meantime, the company lost $1.700, 000 in revenue and intangible customer confidence.

There's no question that the company's CEO sees the strategic importance of technology in executing her business plan, and in this way you share a common basis of principle with her: that IT is a competitive differentiator. However, you believe that diminishing internal IT services risks security and strategic capability, whereas the CEO feels she can acquire that capability immediately and on the cheap through the open market. You're told that CEO Thompson reluctantly agreed to your position if only to pacify COO Willy's concerns.

CORPORATE OFFICE NETWORK TOPOLOGY



You are responsible for a corporate WAN spanning 10 remote facilities and interconnecting those facilities to the central data processing environment. Data is transmitted from a remote site through a VPN appliance situated in the border layer of the routing topology; the remote VPN connects to the internal Oracle database to update the customer data tables. Data transaction from the remote access to the corporate internal databases is not encrypted.

A bulk of the data processing for your company is handled by Oracle database on a high end super computer. The trusted computing based (TCB) internal network is situated in a physically separated subnet. This is where all corporate data processing is completed and internal support team has its own intranet web server, a SUS server, an internal DNS, an e-mail system, and other support personnel workstations. Each corporate department is segregated physically on a different subnet and shares the corporate data in the TCB network.

OTHER CONSIDERATIONS

1. Ever since the article ran in Fortune about GFI, your network engineers report that they've noted a significant spike in network traffic crossing into the internal networks. They report that they cannot be certain what or who is generating this traffic, but the volume and frequency of traffic is certainly abnormal. The management is very concerned over securing the corporate confidential data and customer information.

2. Increasingly, GFI's CEO Thompson attempts to outsource IT competency. In fact, you've been told of a plan from COO Willy to outsource network management and security functions away from your department and to a service integrator. COO Willy warns you that the political environment will only become more contentious over time; you must make a compelling case as to what value your department can bring over an integrator that can provide secure services at 40% less annual cost than you.

3. The interrelationship between data and operations concerns you. Increasingly, some of the 10 remote sites have been reporting significant problems with network latency, slow performance, and application time-outs against the Oracle database. The company's business model is driving higher and higher demand for data, but your capability to respond to these problems are drastically limited.

4. Mobility is important for the organization to interact with the customers and other co-workers in near real-time. However, the CEO is concerned with the mobility security and would like to research for the best practice for mobility computing. The CEO is willing to implement a BYOD policy if security can be addressed.

5. Employees enjoy the flexibility of getting access to the corporate network using a WiFi network. However, the CEO is concerns over the security ramifications over the wireless network that is widely open to the company and nearby residents.

6. The company plans to offer its products and services online and requested its IT department to design a Cloud Computing based e-commerce platform. However, the CEO is particularly concerned over the cloud computing security in case the customer database is breached.

ASSIGNMENTS

- Identify and describe the organizational authentication technology and network security issues.
- Make a list of access points internal and external (remote).
- Design a secure authentication technology and network security for GFI.
- Make assumptions for any unknown facts.
- List all known vulnerabilities you can identify in this environment and address them by proposing a new design. You may use any combination of technologies to harden authentication process and network security measures.
- Address the CEO's concern over the mobility security and design a secure mobile computing (smart phones, tablets, laptops, etc.) in terms of authentication technologies and data protection.
- Identify wireless vulnerabilities and recommend what safeguards, authentication technologies, and network security to protect data should be implemented.
- Design a cloud computing environment for the company with a secure means of data protection at rest, in motion and in process.

Risk Assessment Paper Rubric

You are given a fictional scenario above describing security issues affecting organizational assets. You will identify the risks associated with the assets, and recommend mitigating procedures. You will prepare a **quantitative** / **qualitative** risk assessment to address risk factors on organizational assets. Your final paper will be 15–25 pages long in a Word document and will be graded using the following rubric.

Criteria	Non-compliant	Minimal	Compliant	Advanced
Inventory assets and prioritize them in the order of mission criticality.	Did not inventory or prioritize assets in the order of mission criticality. (1)	Inventoried assets but did not prioritize them in the order of mission criticality. (3)	Inventoried, prioritized assets, but did not address mission objectives in their asset priority. (6)	Inventoried, prioritized assets and addressed mission objectives in their asset priority. (10)
Evaluate enterprise topology and perimeter protection.	Did not evaluate enterprise topology and perimeter protection. (1)	Evaluated enterprise topology but did not include perimeter protection measures. (3)	Evaluated enterprise topology, perimeter protection measures, but did not address mission objectives. (6)	Evaluated enterprise topology, perimeter protection measures, and addressed mission objectives. . (10)
Evaluate remote access to the networks.	Did not evaluate remote access protocols and safeguards to the network. (1)	Evaluated remote access protocols but did not address security safeguards to the network. (3)	Evaluated remote access protocols, security safeguards to the network, but did not address mission objectives. (6)	Evaluated remote access protocols, security safeguards to the network, and addressed mission objectives. (10)
Evaluate authentication protocols and methodologies.	Did not evaluate authentication protocols and methodologies. (1)	Evaluated authentication protocols, methodologies but with insufficient data or inadequate description. (3)	Evaluated authentication protocols, methodologies with supporting data and description, but lacks mission objectives. (6)	Evaluated authentication protocols, methodologies with supporting data, description; and addressed mission objectives. (10)
Assign asset values to organization assets for quantitative / qualitative risk assessment.	Did not assign asset values to organization assets for quantitative / qualitative risk assessment. (1)	Assigned asset values to organization assets for quantitative / qualitative risk assessment but incomplete. (3)	Assigned asset values to organization assets in a complete inventory, but did not address mission objectives. (6)	Assigned asset values to organization assets in a complete inventory, and addressed mission objectives. (10)
Assess vulnerabilities on each asset and impacts if compromised.	Did not assess vulnerabilities on each asset and impacts if compromised. (1)	Assessed vulnerabilities on each asset and impacts if compromised; but incomplete. (3)	Assessed vulnerabilities on each asset and impacts if compromised; of complete inventory but did not address mission objectives. (6)	Assessed vulnerabilities on each asset and impacts if compromised; of complete inventory and addressed mission objectives. (10)
Assess risk based on probability of compromise and its impact discovered on each asset.	Did not assess risk based on probability of compromise and its impact discovered on each asset. (1)	Assessed risk based on probability and its impact discovered on each asset but incomplete. (3)	Assessed risk based on probability and its impact discovered on each asset but did not summarize them. (6)	Assessed risk based on probability and its impact discovered on each asset and summarized them. (10)

Criteria	Non-compliant	Minimal	Compliant	Advanced
Recommend risk mitigation procedures commensurate with asset values.	Did not recommended risk mitigation procedures commensurate with asset values. (1)	Recommended risk mitigation procedures commensurate with asset values, but incomplete. (3)	Recommended risk mitigation procedures commensurate with asset values of complete inventory, but did not address mission objectives. (6)	Recommended risk mitigation procedures commensurate with asset values of complete inventory, and addressed mission objectives. (10)
Formulate 15-25 pages of a quantitative or qualitative risk assessment in APA format.	Did not follow proper quantitative or qualitative risk assessment format, and failed to conform to APA format. (1)	Followed proper quantitative or qualitative risk assessment format but did not conform to APA format. (3)	Followed proper quantitative or qualitative risk assessment format and conformed to APA but insufficient reference list and page count. (6)	Followed proper quantitative or qualitative risk assessment format and conformed to APA in a sufficient reference list and page count. (10)
Executive summary of risk assessment.	Did not include an executive summary. (1)	Included an executive summary but lacks details. (3)	Included an executive summary in details, but did not address the mission objectives. (6)	Included an executive summary in details, and addressed mission objectives. (10)

Risk Assessment Research Paper

The student will research scholarly journal and conference papers and synthesize them to conclude his/her findings about the current security risk assessment problems. The student will:

1. Identify what the current risk assessment problems are.
2. Recommend how to solve these problems identified.
3. Address how to assess the real-time threats, zero-day attacks, advanced persistent threats (APT), Cyberterrorism and other Cyber-attacks.
4. The paper should be in APA format, double spaced, in a minimum of 10 pages. Please use ACM/IEEE journal and conference papers for references rather than any web sites as web sites are unreliable and can be unavailable anytime.

Research Paper Grading Rubric

Criteria					
	Poor	**Fair**	**Good**	**Excellent**	**Percent**
Organization	Sequence of information is difficult to follow. (0 – 7)	Reader has difficulty following work because student jumps around. (8 – 14)	Student presents information in logical sequence which reader can follow. (15 – 22)	Information in logical, interesting sequence which reader can follow. (23 – 30)	30%
Content Knowledge	Student does not have grasp of information; student cannot answer questions about subject. (0 – 12)	Student is uncomfortable with content and is able to demonstrate basic concepts. (13 – 24)	Student is at ease with content, but fails to elaborate. (25 – 37)	Student demonstrates full knowledge (more than required). (38 – 50)	50%
Grammar and Spelling	Work has significant spelling errors and/or grammatical errors. (0 – 2)	Presentation has several and/or grammatical errors. (3 – 4)	Presentation has a couple misspellings and/or grammatical errors. (5 – 7)	Presentation has no misspellings or grammatical errors. (8 – 10)	10%

APA Formatting	Work has significant formatting errors (i.e. references page, title page, spacing, citations). (0 – 2)	Work has several formatting errors (i.e. references page, title page, spacing, citations). (3 – 4)	Work has a few formatting errors (i.e. references page, title page, spacing, citations). (5 – 7)	Work has no formatting errors (i.e. references page, title page, spacing, citations). (8 – 10)	10%