Spring 2024

IS 681-852, 854 Computer Security Auditing

Charles Pak

IS 681 Computer Security Auditing Syllabus

Semester

Course Modality:

This is an online course, which will be conducted fully online, asynchronously via Canvas. For more information on using Canvas and other supported learning tools, visit the IST Service Desk Knowledgebase.

Instructor Information

Instructor	Email	Office Hours
Dr. Charles Pak	cpak@njit.edu	Fridays 10am-12pm by appointment via Webex

*I will respond to all emails/Inbox messages within 24 hours. Discussion posts will be graded weekly. Feedback for project deliverables will be given within a week of being submitted.

General Information

Course Description

This course reflects the current emphasis on information security and security management in Fortune 500 corporations. Students will delve into information protection concepts, privacy impact analysis, computer crime, legal issues, controls and auditing systems, and firewall configuration. Students will have the opportunity to learn and perform evaluations on security infrastructures in a controlled environment in class labs by completing realistic security auditing projects and using vulnerability assessment tools to assess risks and evaluate security controls on networked infrastructures.

Prerequisites/Co-requisites
N/A

Course Learning Outcomes
By the end of the course, students will be able to:

1. Develop an effective internal security audit program.
2. Complete the audit procedures to analyze digital evidence.
3. Create an audit report based on audit practices, analyzing collected data from various operating systems and computing environments.
4. Perform audit data collection from the enterprise networks including the cloud and edge computing.
5. Develop risk management artifacts to communicate with clients to mitigate known risks.
6. Apply audit standards for compliance with industry and government regulations.
7. Conduct research to develop skills to perform audit procedures.

Required Materials

IT Auditing Using Controls to Protect Information Assets by Mike Kegerreis, Chris Davis, and Mike Schiller; Publication Date: September 30, 2019 | ISBN-10: 1260453227 | ISBN-13: 978-1260453225 | Edition: 3rd| McGraw-Hill

* Please note that you will be taking an open-book final exam in this course that uses Respondus Lockdown Browser. Though not mandatory, it's recommended that you purchase the printed version of the textbook. If you choose to purchase the ebook, it's important to make sure you won't run into any issues accessing the book while taking the final exam. Please complete the Respondus Practice Quiz (in Module 2) to make sure Respondus Lockdown Browser and Monitor will work on your computer for the final exam. Should you wish to use the ebook version, please try opening it during this practice exam to make sure you won't run into any issues while taking the final exam. If you encounter any issues, please contact your professor immediately.

Grading Policy
NJIT Grading Legend

Submit all assignments and papers by the specified deadline. 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 Canvas.

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 electronic 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.

Final Grade Calculation

Final grades for all assignments will be based on the following percentages:

Grading Criteria	*Weighted Percentage*
Computer Security Audit Case Study Project Outline	**10%**
Computer Security Audit Case Study Project Paper	**30%**
Recorded Computer Security Audit Case Study Project Presentation and Slides	**20%**
Discussion Forums	**20%**
Final exam	**20%**
Total	**100%**

Course Work

Final Exam (20%): There will be a comprehensive final exam to cover the entire course materials and discussion topics. You will take the final exam online during the final exam period assigned by the instructor.

Discussion Forums: (20% of grade) You are expected to participate in weekly discussion forums in Canvas. When all students participate in a discussion, it creates an active learning environment that will help you better understand the materials and be more successful in the class. You will post your initial response to the prompt by Thursday at 11:59pm and respond to two classmates by Sunday at 11:59pm of the week they are assigned.

Recorded Computer Security Audit Research Project Presentation Slide Deck (20%): This computer security audit case study project presentation will summarize your case study project and present it to your stakeholders (e.g., managers, clients, legal entities, or

the government agency). You will present your case description, activities you performed to discover your findings, the summary of audit evidence and a list of recommendations.

Computer Security Audit Case Study Project Outline:(**10% of grade**) This is one of the first papers you will create to complete your final audit case study project, describing your topic case study topic, description, the problem statement, and detailed audit activities to complete your audit case study project.

Computer Security Audit Case Study Project Report: (30% of grade) There will be a case study project paper with regular milestones. You will have opportunities to iterate and revise your work based on peer and instructor feedback. Students will research a real-world cybersecurity incident case such as the Stuxnet worm attack and create an audit report. Your audit report must include detailed technical background information and describe how the threat compromised the target. The case study paper will be 10-15, double-spaced pages total. The paper should include:

- Security Audit Case Study Topic and Description
- Security Audit Case Study Problem Statement
- Security Audit Procedures Performed using tools, processes, and methods.
- Security Audit Discovery, Findings, Documentation.
- Security Audit Case Study Recommendations
- List of References

Feedback

I will deliver feedback on each assignment using the comments feature in Canvas.

Letter to Number Grade Conversions

A	90-100
B+	85-89
B	80-84
C+	75-79
C	70-74
F	0-64

Exam Information and Policies

NJIT policy requires that all midterm and final exams must be proctored, regardless of delivery mode, in order to increase academic integrity. Note that this does not apply to essay or authentic based assessments. Effective beginning Fall semester 2019, students registered for a fully online course section (e.g., online or Hyflex mode) must be given the option to take their exam in a completely online format, with appropriate proctoring.

Any course that uses online proctoring for exams may require you to do an environmental scan. You are responsible for selecting a location where you are comfortable with yourself and your room being video and audio recorded. You may be asked to use your camera to scan all four walls of the room you are in, as well as the workspace, desk, and area around the computer. Ideally, your exam environment should be well-lit and free from distractions and interruptions.

In this course you will be required to use the following proctoring method to ensure academic integrity for exams:

Respondus LockDown Browser*:* A locked browser used to prevent students from printing, copying, going to another URL, or accessing other applications during an assessment in Canvas.

Policy for Late Work

Late submission must be arranged with the instructor in advance to avoid any penalties imposed by the late submission.

Academic Integrity

"Academic Integrity is the cornerstone of higher education and is central to the ideals of this course and the university. Cheating is strictly prohibited and devalues the degree that you are working on. As a member of the NJIT community, it is your responsibility to protect your educational investment by knowing and following the NJIT academic code of integrity policy.

Please note that it is my professional obligation and responsibility to report any academic misconduct to the Dean of Students Office. Any student found in violation of the code by cheating, plagiarizing or using any online software inappropriately will result in disciplinary action. This may include a failing grade of F, and/or suspension or dismissal from the university. If you have any questions about the code of Academic Integrity, please contact the Dean of Students Office at dos@njit.edu"

Netiquette

Throughout this course, you are expected to be courteous and respectful to classmates by being polite, active participants. You should respond to discussion forum assignments in a timely manner so that your classmates have adequate time to respond to your posts. Please respect opinions, even those that differ from your own, and avoid using profanity or offensive language.

Weekly Expectations

The course is organized into weekly modules. Each week, you will be required to participate in a weekly discussion forum. Initial posts of this discussion forum will be due by Thursday at 11:59pm for the initial post followed by responding to peer posts by Sunday at 11:59pm. As part of the major deliverables, you will be working on a cybersecurity audit case study report and presentation. You will also be taking a final exam at the end of the semester.

Course Schedule

Week	Topic	Reading/Assignment	Due Dates
1	Ch1. Building an effective Internal	Read Ch 1 & 2	Module 1: Peer Introduction & Module Discussion (Initial Post)-Th 11:59pm;

Week	Topic	Reading/Assignment	Due Dates
	IT audit function; Ch2. The Audit Process	Discussion Post for Peer Introductions Discussion Post on Building an effective Internal IT audit function/The Audit Process Article Review	Module 1: Peer Introduction & Module Discussion (Peer Reply)-Su 11:59pm
2	Ch3. Auditing Entity-Level Controls; Ch4. Auditing Cybersecurity Programs	Read Ch 3 & 4 Discussion Post on Auditing Entity-Level Controls/Auditing Cybersecurity Program Article Review Discussion Post on Computer Security Audit Case Study Project Sector Selection due	Module 2: Discussion (Initial Post)-Th 11:59pm. Module 2: Discussion (Peer Reply)-Su 11:59pm Module 2: Discussion-Computer Security Audit Case Study Project Sector Selection-Su 11:59pm
3	Ch5. Auditing Data Centers and Recovery; Ch6. Auditing Networking Devices	Read Ch 5 & 6 Discussion Post on Auditing Data Centers and Recovery/ Auditing Networking Devices Article Review Computer Security Audit Case Study Project Outline-Assigned	Module 3: Discussion (Initial Post)-Th 11:59pm; Module 3: Discussion (Peer Reply)-Su 11:59pm Module 3: Reflection-Su 11:59pm
4	Ch7. Auditing Windows Servers; Ch8. Auditing UNIX and Linux OS	Read Ch 7 & 8 Discussion Post on Auditing Windows Servers/Auditing UNIX and Linux OS Article Review Computer Security Audit Case Study Project Outline-Reminder	Module 4: Discussion (Initial Post)-Th 11:59pm; Module 4: Discussion (Peer Reply)-Su 11:59pm
5	Ch9. Auditing Web Servers and Web applications; Ch10. Auditing Databases	Read Ch 9 & 10 Discussion Post on Auditing Web Servers and Web applications/Auditing Databases Article Review	Module 5: Discussion (Initial Post)-Th 11:59pm. Module 5: Discussion (Peer Reply)-Su 11:59pm Computer Security Audit Case Study Research Project Paper Outline-Su 11:59pm

Week	Topic	Reading/Assignment	Due Dates
		Computer Security Audit Case Study Project Paper Outline Due	
6	Ch11. Auditing Big Data and Data Repositories; Ch12. Auditing Storage	Read Ch 11 & 12 Discussion Post on Auditing Big Data and Data Repositories/Auditing Storage Article Review	Module 6: Discussion (Initial Post)-Th 11:59pm. Module 6: Discussion (Peer Reply)-Su 11:59pm Module 6: Reflection-Su 11:59pm
7	Ch13. Auditing Virtualized Environments;	Read Ch 13 Discussion Post on Auditing Virtualized Environments Article Review	Module 7: Discussion (Initial Post)-Th 11:59pm; Module 7: Discussion (Peer Reply)-Su 11:59pm
8	Ch14. Auditing End-User Computing Devices	Read Ch 14 Discussion Post on Auditing End-User Computing Devices Article Review	Module 8: Discussion (Initial Post)-Th 11:59pm; Module 8: Discussion (Peer Reply)-Su 11:59pm
9	Ch15. Auditing Applications;	Read Ch 15 Discussion Post on Auditing Applications Article Review	Module 9: Discussion (Initial Post)-Th 11:59pm; Module 9: Discussion (Peer Reply)-Su 11:59pm Module 9: Reflection-Su 11:59pm
10	Ch16. Auditing Cloud Computing and Outsourcing Operations	Read Ch 16 Discussion Post on Auditing Cloud Computing and Outsourcing Operations Article Review	Module 10: Discussion (Initial Post)-Th 11:59pm; Module 10: Discussion (Peer Reply)-Su 11:59pm
11	Ch17. Auditing Company Projects.	Read Ch 17 Discussion Post on Auditing Company Projects Article Review	Module 11: Discussion (Initial Post)-Th 11:59pm; Module 11: Discussion (Peer Reply)-Su 11:59pm

Week	Topic	Reading/Assignment	Due Dates
		Computer Security Audit Case Study Research Project Paper-assigned	
12	Ch18. Auditing New/Other Technologies	Read Ch 18 Discussion Post on Auditing New/Other Technologies Article Review Computer Security Audit Case Study Research Project Paper-reminder	Module 12: Discussion (Initial Post)-Th 11:59pm; Module 12: Discussion (Peer Reply)-Su 11:59pm Module 12: Reflection-Su 11:59pm
13	Ch19. Frameworks and Standards.	Read Ch 19 Discussion Post on your Computer Security Audit Case Study Research Findings Computer Security Audit Case Study Research Project Report-reminder Recorded Computer Security Audit Case Study Project Presentation and Slides-assigned	Module 13: Discussion (Initial Post)-Th 11:59pm; Module 13: Discussion (Peer Reply)-Su 11:59pm
14	Ch20. Regulations	Read Ch 20 Discussion Post on Peer Review of Recorded Computer Security Audit Case Study Project Slides Computer Security Audit Case Study Research Project Paper Due Recorded Computer Security Audit Case Study Project Presentation and Slides-reminder	Module 14: Discussion (Initial Post)-Th 11:59pm; Module 14: Discussion (Peer Reply)-Su 11:59pm Computer Security Audit Case Study Research Project Paper-Su 11:59pm

Week	Topic	Reading/Assignment	Due Dates
15	Ch21. Risk Management	Read Ch 21 Security Audit Case Study Research Project Presentation Due.	Recorded Computer Security Audit Case Study Project Presentation and Slides-Su 11:59pm Module 15: Course Reflection-Su 11:59pm
16	Finals Week	Final Exam in Canvas	Final exam due Semester end date, 11:59pm

Additional Information and Resources

Accessibility:

This course is offered through an accessible learning management system. For more information, please refer to Canvas's Accessibility Statement.

Requesting Accommodations:

The Office of Accessibility Resources and Services works in partnership with administrators, faculty, and staff to provide reasonable accommodations and support services for students with disabilities who have provided their office with medical documentation to receive services.

If you are in need of accommodations due to a disability, please contact the Office of Accessibility Resources and Services to discuss your specific needs.

Resources for NJIT Online Students

NJIT is committed to student excellence. To ensure your success in this course and your program, the university offers a range of academic support centers and services. To learn more, please review these Resources for NJIT Online Students, which include information related to technical support.

Discussion Post and Response Evaluation Rubric

Criterion	Unsatisfactory	Satisfactory	Exemplary
Initial Posting			
Relevance	**The posting does not directly address the question or problem posed by the discussion activity.**	**The posting addresses key issues, questions, or problems related to the text and the discussion activity, but in some cases only indirectly or obliquely. It does not apply course concepts fully.**	**The posting directly addresses key issues, questions, or problems related to the text and the discussion activity. The posting applies course concepts well, connecting them to actual course concepts and theories.**
Insight	**The posting does not offer any significant insight, analysis, or observation related to the topic. No knowledge or understanding is demonstrated regarding concepts and ideas pertaining to the discussion topic.**	**The posting does offer some insight, analysis, or observation to the topic but may not demonstrate a full understanding or knowledge of concepts and ideas pertaining to the discussion topic.**	**The posting offers original or thoughtful insight, analysis, or observation that demonstrates a strong grasp of concepts and ideas pertaining to the discussion topic.**
Support	**The posting does not support its claims with either evidence or argument. The posting contains largely unsupported opinions.**	**The posting generally supports claims and opinions with evidence or argument, but may leave some gaps where unsupported opinions still appear.**	**The posting supports all claims and opinions with either rational argument or evidence.**
Responses			
Number of Responses	**The responses do not meet the number required for the discussion activity.**	**The responses fulfill the minimum required number for the discussion activity.**	**The responses exceed the requirement for the discussion activity.**

Criterion	Unsatisfactory	Satisfactory	Exemplary
Substance of Responses	**The responses do not offer any new insight either extending the position of the original post or providing an alternate point of view.**	**The responses generally offer some insight by either extending the point of the original post or offering an alternate point of view, but they may not encourage further thought or reflection on the discussion topic as much as they possibly could.**	**The responses offer either an extension or elaboration on the original posting or a clearly alternate point of view that fosters further thinking, reflection, or response on the discussion topic.**

Presentation Rubric

Criteria	Exemplary (95-100%)	Competent (87-94.99%)	Developing (83-86.99%)	Unacceptable (below 83%)
Depth of Analysis (50% of TOTAL Points)	Response demonstrates an exceptionally in-depth analysis of the theories and/or concepts presented in the course materials to date. Viewpoints and interpretations are consistently insightful and well supported.	Response demonstrates a mostly thoughtful analysis of the theories and/or concepts presented in the course materials to date. Viewpoints and interpretations are usually insightful and well supported.	Response demonstrates a general analysis of the theories and/or concepts presented in the course materials to date. Viewpoints and interpretations are sometimes supported.	Response demonstrates a lack of analysis of the theories and/or concepts presented in the course materials to date. Viewpoints and interpretations are missing, inappropriate, and/or unsupported.
Evidence of Understanding (30% of TOTAL Points)	Response shows consistently strong evidence of synthesis of ideas presented and insights gained throughout the module/course. Clear, detailed examples are provided throughout the paper, as applicable.	Response shows usually strong evidence of synthesis of ideas presented and insights gained throughout the module/course. Clear, detailed examples are usually provided, as applicable.	Response shows evidence of synthesis of ideas presented and insights gained throughout the module/course. Appropriate examples are provided, as applicable.	Response shows no evidence of synthesis of ideas presented and insights gained throughout the entire module/course. Examples, when applicable, are not provided.
Required Components (10% of TOTAL Points)	Response includes all components and meets or exceeds all requirements indicated in the instructions. Each question or part of the assignment is addressed thoroughly.	Response includes all components and meets all requirements indicated in the instructions. Each question or part of the assignment is usually addressed thoroughly.	Response includes most of the components and meets nearly all requirements indicated in the instructions. Each question or part of the assignment is addressed.	Response excludes essential components and/or does not address the requirements indicated in the instructions. Many parts of the assignment are addressed minimally, inadequately, and/or not at all.

Criteria	Exemplary (95-100%)	Competent (87-94.99%)	Developing (83-86.99%)	Unacceptable (below 83%)
Written Communication (10% of TOTAL Points)	Writing is clear, concise, and well organized with excellent sentence/paragraph construction. Thoughts are expressed in a coherent and logical manner. Essentially free of spelling, grammar, or syntax errors per page of writing.	Writing is mostly clear, concise, and organized with excellent sentence/paragraph construction. Thoughts are expressed in a coherent and logical manner. There are a few spelling, grammar, or syntax errors per page of writing.	Writing is somewhat clear, concise, and well organized with good sentence/paragraph construction. Thoughts are occasionally expressed in a coherent and logical manner. There are some spelling, grammar, or syntax errors per page of writing.	Writing is unclear and disorganized. Thoughts ramble and make little sense. There are numerous spelling, grammar, or syntax errors throughout the response.

Research Paper Rubric

Criteria	Exceptional	Proficient	Marginal	Unacceptable
Completeness [5%]	The length requirement for the assignment was effectively fulfilled. Assignment thoroughly addressed all criteria and fully developed and explored concepts.	The length requirement for the assignment was fulfilled. Assignment sufficiently addressed criteria and explored concepts.	The length requirement for the assignment was minimally fulfilled and incompletely addressed criteria and explored concepts.	The length requirement for the assignment was not fulfilled and inadequately addressed criteria and explored concepts.
Depth of Analysis [15%]	Paper demonstrates an exceptionally in-depth analysis of the theories and/or concepts presented in the course materials to date. Viewpoints and interpretations are consistently insightful and well supported.	Paper demonstrates a mostly thoughtful analysis of the theories and/or concepts presented in the course materials to date. Viewpoints and interpretations are usually insightful and well supported.	Paper demonstrates a general analysis of the theories and/or concepts presented in the course materials to date. Viewpoints and interpretations are sometimes supported.	Paper demonstrates a lack of analysis of the theories and/or concepts presented in the course materials to date. Viewpoints and interpretations are missing, inappropriate, and/or unsupported.

Criteria	Exceptional	Proficient	Marginal	Unacceptable
Audit of Incident details of the Adversary Activities [5%]	The Incident details of the adversary activities were comprehensively provided.	The Incident details of the adversary activities were fundamentally provided.	The Incident details of the adversary activities were cursorily provided.	The Incident details of the adversary activities were inadequately provided.
Audit of Security Incident Detection Measures [5%]	Detection measures in place were expertly assessed.	Detection measures in place were realistically assessed.	Detection measures in place were cursorily assessed.	Detection measures in place were inadequately assessed.
Analysis of Failures in Safeguards [5%]	Failures in safeguards in place were expertly analyzed.	Failures in safeguards in place were fundamentally analyzed.	Failures in safeguards in place were cursorily analyzed.	Failures in safeguards in place were inadequately analyzed.
Analysis of Adversary Motivation and Intent [5%]	The adversary motivation and intent were expertly analyzed.	The adversary motivation and intent were proficiently analyzed.	The adversary motivation and intent were marginally analyzed.	The adversary motivation and intent were inadequately analyzed.
Description of Incident Handling Procedures [10%]	The Incident handling procedures were expertly described.	The Incident handling procedures were proficiently described.	The Incident handling procedures were marginally described.	The Incident handling procedures were inadequately described.
Description of Vulnerability Assessment Findings [10%]	The vulnerability assessment findings were expertly described.	The vulnerability assessment findings were proficiently described.	The vulnerability assessment findings were marginally described.	The vulnerability assessment findings were inadequately described.
Description of Major Findings and Lessons Learned [10%]	The major findings and lessons learned were expertly described.	The major findings and lessons learned were proficiently described.	The major findings and lessons learned were marginally described.	The major findings and lessons learned were inadequately described.
Description of Path Forward Security Controls Implemented [5]	The path forward security controls implemented were expertly described.	The path forward security controls implemented were proficiently described.	The path forward security controls implemented were marginally described.	The path forward security controls implemented were inadequately described.
Evidence of Understanding [10%]	Paper shows consistently strong evidence of synthesis of ideas presented and insights gained	Paper shows usually strong evidence of synthesis of ideas presented and	Paper shows evidence of synthesis of ideas presented and insights gained	Paper shows no evidence of synthesis of ideas presented and insights gained throughout the entire module/course.

Criteria	Exceptional	Proficient	Marginal	Unacceptable
	throughout the module/course. Clear, detailed examples are provided throughout the paper, as applicable.	insights gained throughout the module/course. Clear, detailed examples are usually provided, as applicable.	throughout the module/course. Appropriate examples are provided, as applicable.	Examples, when applicable, are not provided.
Writing and Presentation Mechanics [5%]	Complete, well-constructed sentences with faultless grammar, word choice, punctuation, and spelling were written; writing is sharp, coherent, and demonstrates sophisticated clarity.	Complete sentences with mostly correct grammar, word choice, punctuation, and spelling were written; minor errors may exist but do not compromise meaning.	Unclear sentences with significant errors in grammar, word choice, punctuation, and spelling that may compromise meaning were written.	Incomplete, incomprehensible sentences filled with serious errors in grammar, word choice, punctuation, or spelling were written.
Required Components [10%]	Paper includes all components and meets or exceeds all requirements indicated in the instructions. Each question or part of the assignment is addressed thoroughly.	Paper includes all components and meets all requirements indicated in the instructions. Each question or part of the assignment is usually addressed thoroughly.	Paper includes most of the components and meets nearly all requirements indicated in the instructions. Each question or part of the assignment is addressed.	Paper excludes essential components and/or does not address the requirements indicated in the instructions. Many parts of the assignment are addressed minimally, inadequately, and/or not at all.