**Fall 2019**

**Information Assurance Capstone**

**Midterm –** **INFA670 – 9040**

**Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## Instructions

**You are to take this test during the week of October 14 – 20, 2019. It is due on or before 11:59 pm ET on Sunday October 20, 2019. Name your file as follows: LastName\_FirstInitial\_INFA670\_Midterm.**

**Work alone. You may not confer with other class members, or anyone else, directly or by e-mail or otherwise, regarding the questions, issues or your answers. You may use your notes, the open educational resources (OER’s) and the lecture material for this class. If you use the internet it may be interpreted differently from what is in the lectures and class OER’S so use at your own risk.**

**The midterm is worth 25% of your grade for the course. It is scored based on 100 points for the test. The exam is intended to assess your understanding of key concepts in the course. Wherever possible, make sure answers are stated in your own words, and where applicable provide your own examples, rather than repeating the ones used in the course materials. When composing your answers, be thorough. The more complete your answer, the higher your score will be. Be sure to identify any assumptions you are making in developing your answers.**

**While composing your answers, be VERY careful to cite your sources. It is easy to get careless and forget to footnote a source. Remember, failure to cite sources constitutes an academic integrity violation. Use APA style for citations and references. UMUC policies regarding plagiarism will apply for this midterm as well as other deliverables in this course.**

**Do not post questions about this exam in any of the class forums.** If you have a question about the exam e-mail your instructor directly and he will decide whether the entire class needs to be advised regarding the issue or question.

**The test is due no later than 11:59 p.m. Eastern Daylight Time on Sunday October 20th, 2019. Your answers should be contained in a Microsoft Word, or compatible format document uploaded to your Assignments folder. Be sure to put your name on the front of your exam.**

**Late submissions are penalized 20% reduction per calendar day.**

# Exam Questions

**Question 1: Short Essay Answer (32 points).** Please answer in your own words when possible and cite all sources of information. Respond to the following questions considering all the material we have studied in this class for the past 6 weeks. Be specific and fully explain and give reasons for your answer.

There has been reports from the news about a few fatal accidents where software bugs or vulnerabilities were the main source of the problem. For example, in the case of Boeing 737 MAX and 737 NG airplane Maneuvering Characteristics Augmentation System (MCASE) software. In this question we dive into software development lifecycle models and how software bugs can affect the security of the product if not followed properly.

Explain in detail all the software development lifecycle models (SDLC) we discussed in Session 1 and in addition for **each** of the models discuss the following:

1. What are the advantages and disadvantages from a security perspective?
2. What are the strengths and weaknesses of each model from a security perspective?
3. Provide an example scenario of where each one is used from a security perspective.
4. At what stage in the software development lifecycle is security implemented?

**Question 2: Short Essay Answer (32 points).** Please answer in your own words when possible and cite all sources of information. Respond to the following questions considering all the material we have studied in this class for the past 6 weeks. Be specific and fully explain and give reasons for your answer.

Defense Contractor Company X is hiring CyberSecurity experts to help with various security issues regarding their software and hardware teams. You apply to the Principal Cybersecurity position and get called for an in-person interview. The Director of operations schedules a meeting with his existing 30-person team and yourself. Half of the team is on the Contracts and Sustainment teams and half is on the Engineering team and they want to see what you can bring to the table. It is expected that the meeting will turn into a technical discussion and you are expected to brief both teams as expected because you are the Cybersecurity SME (Subject Matter Expert). Their software development team is using the Agile process and they want to add security to this process. The end goal is to reach maturity level 3.

From all the material we covered so far from Session 1 to 5, please provide a detailed answer and full explanation to these questions with enough supporting evidence that can justify full points credit.

1. What security methodology framework should they use to enforce security throughout the software development process?
2. What would you recommend for system network boundary protection from Cyberattacks?
3. What would you recommend for detection of vulnerabilities such as buffer overflows?
4. What would you recommend for C programming language static/dynamic analysis?
5. What would you recommend for wiping out a company mobile device if it gets lost or stolen?

Their hardware team is also trying to certify their Crypto hardware module to EAL 7 and the software team mentioned above is part of this effort as well. The Crypto module uses FIPS-140-2 type encryption algorithm and takes input from an unclassified system and sends the information to a classified system. They need an ATO (Approval to operate) and are in desperate need of a Cybersecurity expert that knows the RMF framework, this is where your expertise comes in. From all the material we covered so far from Session 1 to 5, please provide a detailed answer and full explanation to these questions with enough supporting evidence that can justify full points credit.

1. The Company Director asks – “Explain the RMF framework in detail”?
2. What are the 3 main documents that are required for an RMF evidence package, explain in detail?
3. He also asks, “How do we certify our Crypto module with concurrent certifications, I mean we have the Government ATO - C&A (now A&A) and the EAL 7 certification within almost the same time frame? Explain in detail.
4. Explain the EAL7 certification process in detail?
5. Explain in detail the Vulnerability assessment and analysis methodology you will conduct if we hire you?

**Question 3: Short Essay Answer (36 points).** Please answer in your own words when possible and cite all sources of information. Respond to the following, considering all the material we have studied in this class for the past 6 weeks. Be specific and fully explain and give reasons for your answer.

**This is continuation from Question 2 above.**

You think you did excellent after a good grilling the first day, but the Director was not quite convinced so he decides to bring you in for a second day to cover some more details on how you can help his other teams. This time, a red team of ethical hackers and pen testers gathered in the conference room. Some of them had a few sheets of paper with a lot of questions to choose from just waiting to ask you, but you are confident enough since you have all the experience required for the Principal Cybersecurity position, they are interviewing you for. The Director has a contract with DHS (Department of Homeland Security) and the FBI (Federal Bureau of Investigations) but some of the folks in his team do not have the higher-level clearances DHS and FBI needs but you do.

Please provide a detailed answer and full explanation to these questions with enough supporting evidence that can justify full points credit.

1. What details can you provide us regarding Chinese Malicious Cyber Activity?

Especially, Operation code name Cloud Hopper -

1. What details can you provide us regarding – North Korean Malicious Cyber Activity code name HIDDEN COBRA? Especially

North Korean Tunneling Tool ELECTRICFISH -

North Korean Trojan KEYMARBLE -

North Korean Trojan SHARPKNOT -

North Korean Trojan BANKSHOT -

North Korean Trojan BADCALL -

1. What details can you provide us regarding Russian Malicious Cyber Activity code name GRIZZLY STEPPE?