**ISM 6332 Information Security Risk Management**

**Final Exam – Spring 2023 – 200pts**

**Prof. Jim Jenkins**

**Name:** NICHOLAS CATANI

**You may use the textbook and any material in the class canvas site for this final exam. You may not use any other material, the internet, or communicate with anyone related to this final exam.**

**Please add a statement at the end of this exam confirming your compliance with these requirements.**

**Choose two of the following three scenarios below, answering both the questions within the scenarios paying especially close attention to course content. (Points: 50 pts each scenario / 100 pts total – 500 words max.)**

**Scenario One:**

You have been hired as the Chief Digital Officer at one of the top clothing retailers in the US, who is currently struggling with slowing revenue. Your peers in the C-suite, prior to your hiring, made the decision to expand the company’s online and mobile app presence to open new channels for sales in their quest to stabilize revenue drift. This approach was embraced by the company’s Board of Directors in their last meeting – setting expectations high for these new channels. To be successful in this endeavor, you realize you’ll need to build out your organization’s intelligence infrastructure as the company is woefully behind the curve.

As the CDO, explains how you would balance the desire for this great expansion into digital, against concerns of privacy for your customers.

**Scenario Two:**

You work as the director of risk management for a major regional credit union. Just recently, your organization was hacked by a syndicate who stole personally identifiable information (PII) from your organization, which security experts have alerted you are currently selling on the DarkWeb for $1.00 per record. Given your company’s inability to properly identify and respond to the hack, you have decided to migrate your risk management practice to FAIR and build out a FAIR-based dashboard. In anticipation of unveiling the FAIR dashboard to your credit union’s CEO, you assemble your team to develop a presentation that will address your CEO’s concerns, questions, and issues prior to the meeting.

What are the top questions you need to be prepared for and how do you plan to address them?

* What impact has the attack had on the company’s reputation and how did it occur?

In this case, I would provide an analysis of the hack, the entry point and the vulnerabilities exploited by the cybercriminals, then I would present an extend of the data breach – if any – including the number of affected records and the types of personally identifiable information compromised. I would outline the communication strategy implemented to be clear with members and stakeholders, aiming to rebuild trust and retain reputation.

* How migrating to FAIR framework would improve the company practices?

I would explain its benefits as quantitative framework by emphasizing its structured approach to measuring and evaluating risks, enabling the top management to make informed decisions based on reliable data and analysis. By adopting it, is possible to have a consistent method that assesses risks and enhances resources allocations.

* What is the cost associated with implementing the FAIR framework?

I would discuss the potential cost implications, including any required resources, training, or external expertise associated with it. It is important to convey everything while there may be upfront investments, the long-term benefits of improved risk management would outweigh the initial costs.

* How will the FAIR framework integrate with the existing processes and systems?

I would highlight that the framework can interface with existing registers, incident systems, and other tools, ensuring a seamless flow of information and enhancing the overall risk management ecosystem - without forgetting any concerns on data privacy and security.

**Scenario Three:**

You have just completed your graduate studies at Seattle Pacific University and with your newly minted Master of Sciences in Information System Management or MBA degree and knowledge from this course, you were hired as a full- time information security risk manager at an area hospital. Given the hospital is under the federal regulatory requirements of HIPPA and HiTech (i.e., under penalty of fines and judgments) you know the stakes have never been higher in successfully implementing a solid risk management program.

You have settled on FAIR as your risk management method. Explain what you plan to do during your first 100 days on the job – paying special attention to the challenges of implementing this system in your corporate environment.

My primary focus should be on implementing a solid risk program. Here’s what I would do:

* Assess the existing risk management practices, policies, and procedures.
* Review the current security controls and frameworks in place, identifying any gaps or areas for improvement.
* Conduct an internal awareness campaign to educate stakeholders about the benefits and principles of FAIR framework.
* Highlight the advantages of using this quantitative risk assessment.
* Identify critical assets, systems, and data that require protection, considering the sensitivity of patient health information.
* Define risk appetite and tolerance levels, in alignment with the hospital's overall objectives and compliance obligations.
* Ensure that risk mitigation measures are aligned with industry best practices, including technical controls, policies, and procedures.
* Establish regular reporting mechanisms to communicate risk information to executive leaderships.
* Create risk communication materials for different audiences.

However, implementing FAIR in a healthcare environment shows the following challenges:

* Resources: FAIR requires sustained resources such as specialized training, tools, and expertise. Sometimes hospitals do not have that budget.
* Culture: shifting the risk management approach may require a cultural change within the organization. Resistance to change and misunderstandings can be huge barriers.
* Compliance: it is essential to ensure that the FAIR adheres to the specific requirements outlined in the HIPAA and HITECH regulations.

**Answer each of the following questions below. (Points: 20 pts each question / 100 pts total – 250 words max.)**

1. **What do you think would be the top benefits and drawbacks to risk management utilizing the FAIR method within your company (or at SPU if you are a full-time student)?**

The FAIR framework requires a team to assess threats, estimated loss, and file up questionnaires based on qualitative knowledge. Under that perspective, it is time consuming and money-wise unfeasible, it requires a deep understanding of the FAIR ontology from the team members, uses subjective information that could lead to inaccuracies. Since the framework involves collecting information based on Loss Event Frequency and Loss Magnitude, it often creates a fake sense of certainty due to overreliance on estimations. Also, FAIR focuses on deriving the financial impact of risk using the Montecarlo Simulation model which does not prioritize vulnerabilities, does not lead to actionable steps to improve security posture, and does not provide remediation guidance to manage threats quickly and effectively within the company’s entire network. However, the FAIR model provides protection to break down potential risks and threats into measurable factors while using advanced statistics and probability theory to estimate financial losses in quantitative terms. It allows insiders to make decisions when hard information is lacking based on consistent formulas – for example, RISK = (Threat \* Vulnerability)/Controls.

1. **Explain the process flow for a risk assessment according to Landoll and provide details on you would integrate the mathematics of FAIR to achieve the quantitative analysis.**

There are many security risk assessment methods available and currently in use. Depending on the specific one employed, a security risk assessment may have any number of steps or phases. Landoll’s one comprises the following steps: Project definition, Project preparation, Data gathering, Risk analysis, Risk mitigation, and Reporting.

* Project definition. It is perhaps the most important stage of the risk assessment; it is where the project is going to be scoped and documented. The scope gives a clear understanding of the cost and time of the engagement. Team leaders need to ensure that the project budget and time constraints are well understood and defined between the customer and the team. Then, everything will be documented in a contract.
* Project preparation. It includes both team preparation and planning. In the team preparation, members are selected and notified of the objectives to accomplish during the project. The selection depends on objectivity, experience, and expertise of the person. Whereas in planning, outlines the steps necessary to map the project execution and actions to lead, track, and manage the risk assessment process. Once the lead has confirmed (scope, goals, objectives, deliverables), the project plan with tasks, milestones, and deliverables is created and reviewed with the team.
* Data gathering. The team acquires evidence regarding the security controls in place within the scope of the security risk assessment. It is performed at **administrative level** – policies, procedures, sanction policies -, **physical level** – barriers, physical monitoring, fire safety controls -, **technical level** – automated authentications, authorizations, and computer audit controls.
* Risk analysis. It involves a review of the data gathered and an analysis of the company’s threat landscape to determine the resulting organizational risk. The team must determine the value of assets, the likelihood of threats to the company’s assets, and the existence of vulnerabilities based on the data gathered.
* Risk mitigation. The team must develop suitable recommendations to reduce the identified risks to an acceptable level. Some processes are threat/vulnerability pairs, risk reduction determination, or safeguard cost.
* Reporting. The security team develops a report and a presentation to the project sponsor that clearly identifies the security risks found and recommendations to mitigate those risks. It should provide clear information for the executive, management, and technical personnel.

1. **What are the top three factors you would need to consider when determining the safeguard control for the security architecture of a business system?**

On a basic level, I would consider the CIA triad when determining the security architecture of a business system. It refers to an information security model made up of the three main components: confidentiality, integrity, and availability. Each represents a fundamental objective of an information security system.

* **Confidentiality**: It is often associated with secrecy and the use of encryption. Generally, the data is only available to authorized parties and cannot be compromised by unauthorized agents. Ensuring confidentiality means that information is organized in terms of who needs to have access and its sensitivity.
* **Integrity**: Data is not tampered with or degraded during or after submission. Also, it is certain that the data has not been subjected to unauthorized modification, either intentionally or unintentionally.
* **Availability**: The information is available to authorized users when it is needed. A system when is available, it must have functioning computing systems, security controls, and communication channels. Also, it must be resilient against cyber threats, and have safeguards against power outages, hardware failures, and other natural disasters – earthquakes – that might impact the system availability.

1. **Explain how the ontology for risk management and control structure for an organization are related and why the relationship between them is important.**

The ontology for risk management and the control structure of an organization are complementary. The ontology establishes a common understanding and categorization of risks, while the control structure defines the controls and mitigation measures to address those risks. The relationship between them ensures a systematic and comprehensive approach to risk management, supports informed decision-making, promotes consistency, and facilitates effective communication throughout the organization. An example in risk identification and assessment… the ontology helps in systematically identifying and categorizing different types of risks based on their nature, causes, and potential impacts. It provides a taxonomy or classification scheme for risks. The control structure, informed by the ontology, then outlines the specific controls and mitigation measures that should be implemented to address each identified risk. By aligning the control structure with the ontology, organizations can ensure comprehensive coverage of risks and the appropriate controls to manage them effectively.

1. **Through your investigation of** **NIST RMF, OCTAVE, TARA, COBIT FAIR risk management frameworks, security architecture, threat modeling (e.g., Att@ck), and governance – how do you think these all fit together in the context of this course?**

If we look at the syllabus, the objective of this course is to provide a deeper understanding of the components and issues in security risk management and a list of objectives follows. I think the course is founded on learning cyber procedures. On a closer look, for example, security architecture and thread modeling are cyber procedures, the former helps designing computer systems to assure the security of the company underlying data – the foundation of defense against security threats. Whereas the latter is a procedure for optimizing application, systems, or business process security by identifying objectives and vulnerabilities first, and then defining countermeasures to prevent or mitigate the effects of threats to the system.

**Grade Question 250 words:**

This was a course of exploration into the world of information security, risk management, and privacy. Do you feel you learned what you expected in the class? Based on your learning, what grade do you feel you deserve in the class? Explain and make the case that you have earned this grade!

This course gave me the opportunity to learn the foundations of a risk assessment, design from scratch a risk dashboard to track the assets, vulnerabilities, security measures, and control for a European Bank, create and keep a podcast to document my learning experiences – something I have never done before -, and apply statistics to cybersecurity activities. Asking to choose a grade might be hazardous because the yardstick between me and Professor Jenkins differs widely – his experience and knowledge is far beyond my understanding of the subject. However, since I joined SPU, I’ve always pushed myself over the limits to get good grades. My lowest grade after 10 courses is an A-. Thus, everything from an A- up is considered a good job from my perspective. Eventually, a good GPA will help me to get into a PhD program next year. Now, there are several reasons why I would like to get at least an A- in this course.

* Citizenship: expect a couple of cases, I have shown active participation during classes asking questions, giving my contributions to the class, and keeping up with the class assignments – the isolated case happened when I asked a small extension for the final exam.
* Good Team member: gave my contribution to the team project with an open-minded attitude by supporting the others when necessary and giving ideas to craft the final video.

From a course content perspective, I had the chance to master and pinpoint different characteristics of qualitative and quantitative risk analysis – one of my favorite podcasts I have made in the past weeks.

