**CIS-481: Introduction to Information Security**

**InfoSec Chapter Exercise #4 - Option B**

**Team: Project Team 11**

**Names: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson**

**Logistics**

1. Get together with other students on your assigned team in person and virtually.
2. Review the two options available and decide on only one to pursue as a team.
3. Discuss and complete this assignment in a collaborative manner. Don’t just assign different problems to each teammate as that defeats the purpose of team-based learning.
4. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

**Problem 1**

Review the *Bank Solutions Disaster Recovery and Business Continuity* teaching case linked below [Camara, S., Crossler, R., Midha, V., & Wallace, L. (2011). Teaching Case: Bank Solutions Disaster Recovery and Business Continuity: A Case Study for Business Students. Journal of Information Systems Education, 22(2), 117-122.]

<http://jise.org/Volume22/n2/JISEv22n2p117.html>

The intent of the case is to give students an opportunity to gain real world experience with a theoretical concept that can be difficult to comprehend fully. At the conclusion of this case, students should possess a greater understanding of the critical decision-making process that goes into analyzing and deciding what risks need to be dealt with as a part of a Disaster Recovery and Business Continuity (DR/BC) team. To accomplish the stated goal of this case, information from a fictional company, Bank Solutions, Inc., is provided. Bank Solutions, Inc. is a provider of item processing services to community banks, savings and loan associations, Internet banks, and small- to mid-size credit unions. As members of the engagement team performing the risk assessment, your team has been given the task of assessing Bank Solutions’ incident handling, business continuity, and disaster recovery strategy.

Each group of students will work as a member of an engagement team in charge of performing the incident handling, DR/BC risk assessment for Bank Solutions. Each group should read the case background and the facts identified in the interviews.

Together as a group, prepare a report of recommendations for correcting each of the identified conditions (thereby addressing the risks) from the assigned subset of facts given to you by your instructor. Prepare to discuss your results in class. You should be ready to explain and elaborate on why you identified each condition and each risk. Highlight the changes you recommend to their IR/DR/BC contingency plans. *(50 points)*

**Answer:**

In order to make a risk assessment report of recommendations for incident handling, business continuity and disaster recovery which leads to make a unified solution, first of all we would get compliance of CMMC, ISO 27001 and GDPR, to ensure better data security standards all over the Bank Solutions’ the company should focus on how to implement on CIA Triad, to secure the organization’s sensitive data from phishing and cyber hacking. Complete trainings and incentives should be provided to employees to get safe from social engineering’ attacks. Moreover, backup files should be ensured so that in case of data phishing an organization wouldn’t lose its data. Secondly, the organization shouldn’t store all of its’ data in a single software, but it should be divided in different software's, so that in case of attack, data from one data security. As per the given articles Bank solutions has defined the type of solution it needs for risk management, incident handling, business continuity and disaster recovery.

* As per reflecting on other bank entities of United States of America, they are following Gramm-Leach Bailey FI Act 2020, that the highly sensitive information couldn’t be shared to any third party. Only those can access the data, which are considered as high authorities of the organization.
* In order to focus on contingency planning, the only thing, which is under my perspective is that all these planning's should be dynamic. It should vary from time to time. The company following old contingency planning’s could not make it when it comes to securing digital assets of an organization, the company should follow the guidelines, under CMMC compliance and should hire cloud engineers, penetration hackers and information security experts to cope with all situations and immediate decision making.
* Whenever it comes to specificity, task integrity is what actually matters. The banking officials aren't liable form time bracket of 9-5, they should overlook the task whenever it is necessary for them too, the task’s expressed should be done by adhocracy. Planning, testing's, backup’s, documentation. All these are core task’s and task handling led to operational excellence.
* If plans are missing, the task should be divided amongst all the team, human efficiency matters more than that of machine learning. All the organizational vulnerabilities, threats/ attacks and problem should be discussed and troubleshoot by mutual meetings all the suggestions should be overlooked and the best should be implemented across the organization.