BCYB 640 – “ERM IN ACTION” CASE STUDY

Exercise Questions

1. **What does the organization need to do?**

   It is imperative that the firm begin by creating a thorough risk management plan. Internal controls and governance need to be strengthened in light of the rising incidence of security incidents, particularly in retail banking. Prioritizing security updates is necessary to stop these attacks from affecting operations. Additionally, it's critical that they fortify their risk culture, which entails raising leadership participation, awareness, and training levels in risk management. Furthermore, more robust digital security measures are needed to protect sensitive data in light of the transition from paper to digital records. Enhancing uniformity and productivity among their international teams may be possible with the integration of IT operations via business platforms.

2. **What types/categories of risk is the organization dealing with?**

   The organization is exposed to a variety of dangers. They face operational and cybersecurity risks as a result of problems with updating and maintaining their IT systems, as well as security incidents and data breaches. Because companies have to deal with numerous intricate international regulations and their internal compliance management processes are still in their infancy, there is also a significant risk of regulatory compliance. Additionally, there is a rise in the risk of fraud, particularly in relation to identity theft and mortgage fraud. In addition, there are governance risks brought on by a lack of strong executive control and strategic risks associated with their digital transition. They even have vendor risk because they contract out a portion of their services and infrastructure.

3. **Where does the management team start? What approaches could they take?**

   To begin with, the management team should identify and rank the most significant risks through a thorough risk assessment. After that is established, they must provide executive oversight by putting in place a risk governance architecture that clearly defines roles, responsibilities, and reporting channels. It's also critical that they prioritize resolving the most serious problems first, such as strengthening security procedures, streamlining compliance procedures, and increasing internal controls. It's also critical to strengthen the organization's risk culture. To make sure that risk management is included into day-to-day operations and business choices, they could make use of an enterprise risk management (ERM) framework.

4. **As the CEO, what risks are you most concerned about? What value would better understanding and managing risk have for the organization?**

   As the CEO, I would assume that the most urgent issues are operational disruptions brought on by security incidents, as these can undermine consumer confidence and compromise business continuity. Failures to comply with regulations would also be concerning because they could result in large fines and damage the bank's reputation. An other significant worry would be the rise in fraud, especially identity theft and mortgage fraud, which can cause losses in terms of money and reputation. Finally, you should address the governance gap that may be impeding the organization's capacity to successfully manage these risks. An improved understanding of risk can help the company become more resilient. This entails having the ability to minimize the effects of incidents and react swiftly to threats. Effective risk management also helps the bank avoid expensive compliance problems, preserves its reputation, and makes sure resources are directed where they are most required.

5. **As CIO, what risks are you most concerned about? What steps do you & the IT team need to take?**

   Given the rising number of security incidents, cybersecurity risks would probably be your top concern as the CIO. Maintaining antiquated systems without regular upgrades and maintenance puts a great deal of operational risk because it can cause disruptions. When moving from paper to digital records, you would also be concerned about data breaches that might reveal private client information. Me and the IT staff should concentrate on bolstering security measures by purchasing cutting-edge technologies like intrusion detection systems, firewalls, and encryption to address these. Patching and updating the system on a regular basis is crucial to preventing vulnerabilities. To reduce downtime in the event that a breach does occur, you would also need to create and practice incident response plans. Furthermore, it's critical to control vendor risks by making sure outside suppliers adhere to strict security and privacy regulations.

6. **What role does an organization’s “culture” play in risk management?**

   Culture has a significant impact on risk management. Employees are more likely to follow procedures correctly, report suspicious activity, and take preventive action when there is a risk-aware culture in place. Everyone, from management to employees, benefits from a strong risk-aware culture that makes risk management part of their job description. Additionally, it promotes accountability by making sure people understand their part in risk mitigation and reporting. When risk management is ingrained in the company's culture, it becomes a routine aspect of operations, which can reduce incidents and strengthen the organizational response in the event that something goes wrong.