BCYB 640 – "ERM IN ACTION" CASE STUDY

Situation

A global bank has operations in more than 50 countries, and over 125,000 employees across the globe. IT teams are co-located within each facility to more directly support global and local lines of business. Some functions, infrastructure and services are performed internally, and others outsourced to vendors.

Issues

The bank is dealing with pressure on several levels:

1. The bank has experienced growing number of security incidents in the past year, each of which have significantly impacted bank operations for multiple days. IT is also struggling to maintain and upgrade several critical systems, and consolidate certain functions via enterprise platforms and services.

2. Recent audit findings revealed a fundamental breakdown in internal controls and processes related to retail banking functions. Findings specifically cited weakness in risk culture, awareness, training, Immature processes for assessing and testing regulatory compliance, executive-level risk governance and oversight.

3. The global digital economy and desire to reduce operating costs are pushing paper records to digital, generating concerns about access and data safeguards.

4. The bank deals with a challenging compliance landscape. Over $1.1 trillion is spent to comply with US federal requirements, and there are over 10,000 regulations worldwide. At the time of writing, there were new regulations in the pipeline.

5. The industry has seen a proportional rise in all categories of fraud over the recent decade, along with a significant rise in mortgage fraud arising from easy credit.

6. The emergence of an underground economy monetizing stolen identities, illegal transactions, phishing and other financial crimes are causing losses.

Challenge

Management recently began discussing revamping their risk management approach to assure common governance and assurance processes across facilities and teams.

The CEO has directed your management team develop a comprehensive plan to identify and reduce risks that affect critical operations.