## Identify the essential elements of risk associated to new technology.

The main issue that occurs when a new technology is introduced is change management risk. There should be a proper set of guidelines or documentation before implementing any new technology in the organization.

Introduction of new technology will create the need for training employees and studying the impact it creates on existing workflow. Requirement for skilled employees will increase and this is a risk Smithsonian bank must address.

New technology introduction in financial institution always welcomes scrutiny from customers. If Smithsonian bank establish proper trust between customers accepting the new technology inception, then the result can boost the future business plans of the bank. If not, there will be negative consequences from the customers and will have hard time to gain customer trust.

A new technology must always meet the hardware and software requirements/capabilities to integrate properly in the current organization business requirements. Also risk of new operational issues can be possible when integrating a new technology.

New technologies must be compliant with the regulatory requirements and policies. In a financial institution all the technologies that deal with card payment must comply with PCIDSS.

Allocation of resources to the new technology can be challenging and this risk needs to be mitigated before implementing new technology.

## Identify the key required goals and practices for the bank's Internet banking technology and products.

In internet banking technology the main aim is to maintain the privacy of customers' data. This is one of the important practices that every organization must follow and company should have response management team to solve issues regarding any privacy related issues.

Security availability must always be in high priority. Internet banking must always try to aim 24/7 operation hours for any unforeseen security adversities.

Smithsonian bank can reach out to other part of the world than Africa as the global reach using internet banking can potentially provide more business opportunities.

Alert management systems: It is important to maintain authorization standards of user management in the internet banking. The management should make sure that all the controls are well maintained. An alert system should be implemented to notify any deviations form standards and record the logs of every attribute regarding to the incident for future audit purposes.

Bank must also indulge in customer awareness programs to educate customers over new technologies and products and how to use safely and emergency information when in need. All these will help to ensure customers can identify any issues from their side.

The board of directors and senior management should ensure that company is maintaining proper storage mechanisms for the customer data. It is must that Smithsonian bank provide reasonable assurance to customers on the integrity of the data.

## Gather information regarding the Internet banking objectives of the bank, the strategy used to achieve the objectives and the way that the bank is using Internet technology in the relationships with its customers.

- Implementing stringent security measures on customers privacy data
- 24 hrs availability of internet banking facilities to access their accounts that enable them to perform transactions.
- Internet banking will enable users to visit company website more often which in turn generates more traffic to the websites and usage of bank apps will reduce the need to go for physical locations where maintenance cost is more.
- Since bank opted for external audit for providing reasonable assurance to all the stakeholders, this move by the bank is positive in customers and their trust on the bank.
- Since investment from the bank is high, this shows that the bank is involving more in its operations and development which in turn increase the trust of the customers.
- Bank informs that it is compliant with the Banking Act, FICA, Credit Act and more compliances which are in the industry for a financial institution. This will provide credibility for the bank.
- Important strategy to maintain objectives is by continuous improvement by regularly evaluating and enhancing internet banking platforms to incorporate new technologies.
- The bank ensures transparency and judgement and meets regulatory needs globally and internationally.

## Prepare a nearly complete list of areas of review.

- Daily transactions involve using the banking internal network used by customers and banking, this interactive function provides highest risk to any organization and requires strong controls.
- Risk management should be reviewed according to the COBIT5 framework.
- Review of personal responsibilities and accountability must be done in accordance with their access levels. Everyone in the organisation especially board of directors and senior management must involve in segregating of duties for historical records.
- Introduction of alert management should be reviewed with all the possibilities and there should be controls.
- Review of compliances regularly is must in a financial organization like Basel II banking practices, the Banking Act, FICA, Money Laundering, Access to Information, USA Patriot Act, Conflict of Interests, Credit Act, and King III.
- Review of duties across organizations and their responsibilities is must and this should be taken by higher management and board of directors to ensure authorized personal are doing their respective tasks while monitoring is in place.
- Review of backup, disaster recovery plan should be done regularly. In a financial institution it is very important to maintain 24 hrs service to customers.
- Business strategies must also be reviewed constantly to ensure all the services/process are up to the market standards and organization goals are achieved.
- Regular review of data integrity is must in a financial organization as the customer data is very sensitive and proper backups are available in an offsite location.
- Review of existing controls in place already and their efficiency over the past period.
- Review of all the virus detection and prevention controls that exists and reviewing the protocols that deal with DDOS attacks and similar attacks in internet banking facilities.

References:

https://www.isaca.org/resources/cobit