Case Study 3 & 4: Bank Risk Assessment

Table of Contents

Executive Summary

CIS Bank operates as a large scale international bank with branches across North America, South America, and the Middle East. Following market trends, CIS Bank is interested in expanding their Mobile Banking department which currently only operates within 30 miles of CIS Bank headquarters. All of core systems of CIS Bank are located in the Midwest United States. Before expansion of the mobile application nationwide, CIS Bank has hired NKM consulting to conduct a risk assessment in order to gage how much risk they are currently working with and if the controls currently in place are adequate to mitigate this risk.

The following risk assessment evaluated the risks facing all the systems within CIS Bank: Core Banking, Mobile Banking, Phone Banking, and Internet Banking as well as risks associated with internal CIS Bank systems including: Workstations, Desktops, and Laptops.

This risk assessment considered knowledge from:

- Risk profile of each asset
- Previous risk assessments
- Likelihood of Threats to the asset
- History of potential costs threats may create
- History of financial costs for controls

The risk assessment found that the most critical assets for CIS Bank are **Internet Banking,** and **Core Banking**. **Internet Banking** had the highest **Threat Score** and **Inherent Risk Score.** Overall, **Desktops** have the **least** **Residual Risk** and even though **Internet Banking** has the **highest** **Control Score**, it still has the **highest** **Residual Risk.**

The results of this risk assessment show that the current controls in place for mitigating the risks at CIS Bank are inadequate. This can be seen in the residual risk score for one of the most critical assets, **Internet Banking**, where the controls in place are only reducing the inherent risk by approximately 28%.

Moving forward, it can be concluded that managing the Internet Banking system should be made a top priority of CIS Bank to ensure its high-risk rating is mitigated in such a way that it does not overwhelm the resources of the bank. A possible solution could be to remove some of the controls from another asset in order to place more on high risk assets such as internet banking. Furthermore, seeing as the Mobile Banking system is still in the infancy stage and is only available to customers residing within close proximity (30 miles) to the bank's headquarters it will be important to continue to roll out adequate security measures as its grows beyond regional borders.

Method

To find the overall risk of CIS Bank after considering current controls, residual risk, a risk assessment with the following steps was conducted:

1) Values for the quantitative model for CIS Banks risk assessment were created by senior management. Instead of completing a business impact analysis, the team decided to use a general baseline to save time. These generalized numbers provide approximate residual risk data for the banks information system assets.

2) CIS Banks risk profile was created by providing a questionnaire to all key personnel in each of the assets. Questions consider Financial, Legal, Reputational, and Regulatory implications and how they impact the Confidentiality, Integrity, Availability, and Accountability (See Appendix B). Each of the questions were assigned a hidden quantitative value associated with their sensitivity. Results were compiled into a table and averaged to produce an Asset Criticality score. With this score in mind, recommendations as to which of the environments need to be prioritized can be made

3) Using data gained from a third party cyber intelligence company a threat universe for each asset is determined. Information is collected on current threats, information regarding current threat actors and examining previous threats is used to create a quantitative score. This quantitative score represents likelihood of the threat occurring as well as the impact, monetary damage, if the threat occurs to the asset. The overall Threat Score is computed by multiplying the likelihood and impact scores. The overall raw risk for each of the assets (Inherent Risk) is then calculated by multiplying the Threat Score by the Asset Criticality.

4) The controls provided for each asset were evaluated by considering how much they mitigate the current threats the asset it facing. Controls are then evaluated based on how well they have mitigated specific risks in the past, the maximum likelihood of it mitigating future threats, and the maximum amount of money it could save the bank in the future. Due to the fact that a business impact analysis was not conducted we can only give a rough estimate of likelihood and monetary impact. Likelihood and monetary impact also depends on the severity of the risk which also depends on the situation.

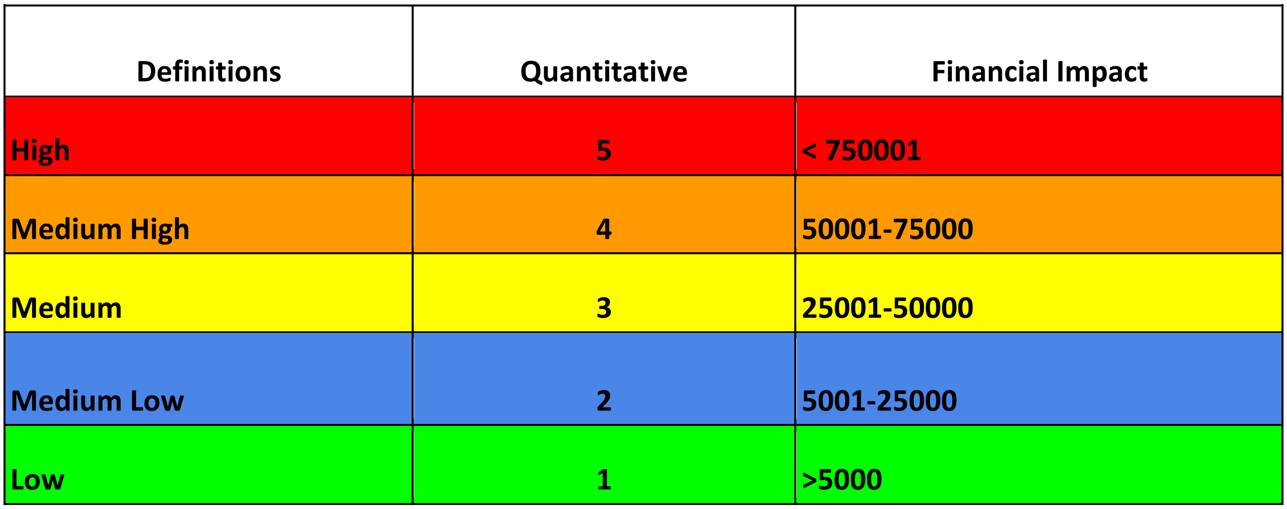
5) In conclusion, taking the Inherit Risk Score minus the Control Score gives the Residual Risk Score for each of the assets. From here, CIS Bank can see how much uncontrolled risk it has left to manage and recommendations can be made regarding additional controls as well as how to disperse controls among the assets.

Conclusion

While this risk assessment provides a good general overview of each of the assets, it lacks the ability to give a detailed analysis on what type of threats the asset might face in order to get a better idea of the type of controls needed to mitigate this risk. More detail can be included by incorporating a quantitative model, combining both a quantitative model with a qualitative model can lead to better results. Moving forward, a quantitative model should be based off a business impact analysis to help get specific numbers and accurately assess how much a threat will cost CIS Bank and in turn allow for the proper control to be put in place.

It is also important to understand that each system of the bank works together, this means that a security flaw in one asset could cause damage to the rest of the assets. As mentioned above, the threats should be more specific as the generalization of them makes it harder to attribute how much each control mitigates them. This would allow the analyst to better evaluate how each control relates to each other not only in its own asset but in other assets. Depending on the interoperability of the assets this can be an important consideration.

Appendix A



Definitions	Quantitative	Financial Impact
High	5	< 750001
Medium High	4	50001-75000
Medium	3	25001-50000
Medium Low	2	5001-25000
Low	1	>5000

Appendix B

Confidentiality, Integrity, Availability, Accountability Table	
Confidentiality	The consequence of unauthorized disclosure or compromise of data stored, processed, or transmitted by the resource.
Integrity	The consequences of corruption or unauthorized modification/destruction of data stored, processed, or transmitted by the resource.
Availability	The consequences of loss or disruption of access to data the resource stores, processes, or transmits.
Accountability	The consequences of the inability to hold users accountable for their actions in the resource.

Appendix C

Terms	Definitions
Inherent Risk	The amount of risk a business has with the current controls.
Residual Risk	The amount of risk left over after controls implemented by the risk assessment.
Asset Criticality	Determining the asset that needs to be addressed first.