Colin Monroe

Executive Summary

Bank Z is an international bank and is interested in expanding their Mobile Banking department. While, Bank Z is an International Bank, all of its core systems are located in the midwest of the United States. In order to determine if additional funding will be required to expand Mobile Banking a risk assessment is being conducted to see if the current risk is being managed adequately.

This risk assessment took into account knowledge from:

- Risk profile of each asset
- Previous risk assessments
- Likelihood of vulnerability / threat pairings to the asset
- History of potential costs threat events may create
- History of financial costs for controls

This risk assessment shows that the most critical assets for Bank Z 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 shows that the current funds allocated for mitigating the risks for Bank Z is inadequate. This can be seen in the inherent risk score for one of the most critical assets, Internet Banking. Where the controls that can be afforded are only mitigating approximately 28% of the inherent risk of the asset. Therefore, Bank Z should look to

invest in **Internet Banking** more than other assets in order to manage the risk. This should be done before moving onto expanding the Mobile Banking asset.

Method

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

1) The values of the quantitative model for this risk assessment were created by senior management. While normally these values are created through a business impact analysis due to time constraints senior management decided to use a general baseline. While not completely accurate it allows Bank Z to gather approximate residual risk data on their information system assets.
2) The risk profile was created by conducting a questionnaire for all key personnel in each system. Questions were created by taking into consideration Financial, Legal, Reputational, and Regulatory implications and how they impacted the Confidentiality, Integrity, Availability, and Accountability (Appendix B). The answers to the questionnaire were then given a hidden quantitative number rating for their sensitivity. These results were compiled into a table and then averaged to produce the Asset Criticality. This allowed a recommendation to be made for which environment needs to be prioritized.
3) The identification of the threat universe for each asset was conducted using knowledge gained from third party cyber intelligence companies, data regarding previous and current threats, information regarding current threat actors and examining the threats the company has faced previously. This information was then used to create a quantitative score, see appendix A, for the likelihood,

probability of occurrence, and impact, monetary damage if a threat was to occur. The overall Threat Score was then created by multiplying these two values. To calculate the overall raw risk for each asset, Inherent risk, the Asset Criticality is multiplied with the Threat Score.

4) The current controls for each asset were evaluated by taking into consideration how much they mitigate current threats. This was determined by comparing how well each control has historically mitigated specific threats, the likelihood of it mitigating future threats, and how much they can possibly save Bank Z monetarily. These considerations were converted into a quantitative score for reduction in probability and impact. Both scores were then multiplied together to give an overall control score for each asset.
5) Finally the Inherent risk score minus the Control score gave us the Residual risk score for each asset. This allows Bank Z to see how much residual risk, uncontrolled risk, it still has left to manage.

Conclusion

While this risk assessment allows for a good general overview of each of the assets it lacks granular analysis. Incorporating a quantitative model can be a good idea however combining it with a qualitative model may lead to better results. The quantitative model also needs to be based off of a business impact analysis to help get better specific numbers. The risk assessment should include a more holistic approach to gathering information for its Asset

criticality. This should be done by incorporating interviews, group sessions, and observation of the environment. 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. Overall the most important information in a complete quantitative analysis is historical data which was lacking in this assessment.

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.**