Initial Plan (Still subject to changes):

As the newly hired CISO of one of the largest Universal Banks in the Philippines, I understand the importance of establishing and maintaining a comprehensive and effective information security program to protect the bank's information assets and technologies. Given the diverse range of products and services offered by the bank, as well as its focus on digital transformation, it is critical that a robust and comprehensive security program is in place.

To fulfill the CEO's expectations and ensure the success of the information security program, I will follow a step-by-step process:

Conduct a Risk Assessment: The first step in establishing an effective information security program is to conduct a thorough risk assessment. This will involve identifying the bank's critical information assets and the risks to these assets, as well as evaluating the current security controls in place to protect these assets. This information will be used to prioritize the security initiatives and resources required to effectively protect the bank's information assets. The risk assessment will focus heavily on Online and cloud based threats since these are the largest platforms where transactions will take place and therefore where attackers would target.

Develop a Security Strategy: Based on the results of the risk assessment, I will develop a comprehensive security strategy that will outline the bank's vision, mission, and objectives for information security. This strategy will be aligned with the bank's overall business goals and will provide a roadmap for the implementation of the information security program. I will also make sure that the strategy takes into account the

possible threats and vulnerabilities the bank system may encounter. This will ensure that the banks will experience less to no number of attacks during its run.

Implement Security Controls: The next step will be to implement the necessary security controls to protect the bank's information assets. This will involve the deployment of technical security controls such as firewalls, intrusion detection systems, and encryption, as well as administrative and physical controls to ensure the confidentiality, integrity, and availability of the bank's information. Since the largest number of transactions will occur the bank's online platform, cloud platforms, and ATMs, I will allot a big chunk of the resources given for bank security in these areas.

Develop a Disaster Recovery Plan: To ensure that the bank is prepared for any potential security incidents, I will develop a comprehensive disaster recovery plan. This plan will outline the procedures and resources required to respond to a security incident, as well as the steps to be taken to minimize the impact of the incident and restore normal operations.

Train and Awareness: To ensure that all employees are aware of the importance of information security, I will develop and implement a training and awareness program. This program will educate employees on the bank's security policies and procedures, as well as best practices for protecting the bank's information assets.

Monitor and Evaluate: The final step in establishing an effective information security program is to monitor and evaluate the program on a regular basis. This will involve conducting periodic risk assessments, evaluating the effectiveness of the security controls in place, and making

any necessary adjustments to the security program to ensure that it remains relevant and effective.

In conclusion, as the CISO of the largest Universal Bank in the Philippines, I am committed to establishing and maintaining a comprehensive and effective information security program to protect the bank's information assets and technologies. By following the step-by-step process outlined above, I am confident that I will be able to fulfill the CEO's expectations and ensure the success of the information security program.