Initial Plan (Still subject to changes):

Step 1: Evaluate the present state of information security at the bank.

- Examine existing security policies, methods, and technologies.
- Determine the gaps and areas for improvement.
- Determine the risk levels of existing systems and applications.

Step 2: Create an all-encompassing information security strategy.

- Align the strategy with the overarching goals and objectives of the bank.
- Take into account industry best practices and laws.
- Define critical components like risk management, data security, and incident response.

Step 3: Create a comprehensive action plan.

- Determine the importance of initiatives based on their risk and business impact.
- Distribute resources (e.g. budget, personnel)
- Create project timetables, milestones, and objectives.

Step 4: Put security measures in place and track progress.

- Implement specific initiatives
- Put in place security measures such as firewalls, encryption, and multi-factor authentication.

- In order to measure success and identify areas for improvement, establish regular monitoring and reporting mechanisms.

Step 5: Inform and educate.

- Make certain that all staff understand the significance of information security.
- Provide training and education programs
- Develop a security culture throughout the organization.

Step 6: Constantly evaluate and improve

- Evaluate the efficiency of security measures on a regular basis.
- Keep an eye out for new dangers and adjust your security strategies accordingly.
- Improve processes, technologies, and personnel education on an ongoing basis.