INSY7314

ICE TASK 2

Kayla Ferreira
ST10259527 | VARSITY COLLEGE

Table of Contents

Q1.

The SWIFT network helps banks send secure messages to each other when doing cross-border transactions. It does not move money itself but makes sure payment instructions are sent quickly and correctly using unique codes (BICs) and standard formats like ISO 20022. For example, if a bank in South Africa wants to send money to a bank in Germany, it uses a SWIFT MT103 message to pass on the payment order safely.

The advantages of SWIFT are that it connects over 11,000 institutions worldwide, provides strong security and reliability, reduces errors through standardization, and helps banks meet compliance rules such as anti-money laundering (AML). It is also more efficient than older systems like fax or telex.

However, there are some limitations. SWIFT only sends messages and does not settle the money itself, which can cause delays since it relies on correspondent banks. It is also expensive, especially for smaller banks, and can be used as a political tool when certain countries are cut off. In addition, it is not as fast as newer technologies like blockchain-based payments and has faced cyberattacks, such as the Bangladesh Bank incident in 2016.

Q2.

International banks use many security measures to protect against cyber threats. Encryption is used to protect data both in transit (using TLS) and at rest (using AES-256). Multi-factor authentication (MFA) adds extra protection by using passwords together with biometrics or tokens. Secure APIs and tokenization protect sensitive information like card numbers. Banks also use fraud detection systems, AI, and real-time monitoring tools to stop suspicious transactions.

To protect data integrity, banks use hashing (like SHA-256) and digital signatures so data cannot be changed. Confidentiality is maintained with role-based access control and end-to-end encryption. At the same time, banks must follow international regulations. These include GDPR in Europe, POPIA in South Africa, PCI DSS for card data, Basel III for risk management, and FATF standards for fighting money laundering and terrorism financing.

In short, SWIFT provides secure international messaging for banks, but it has some limits. Banks therefore use advanced security tools and follow strict regulations to make sure data stays safe, private, and compliant across borders