Steven Bomela
St10304166

INSY7314

Q1. SWIFT in International Banking

Overview

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a global network that enables financial institutions to exchange standardized financial messages securely. While it does not transfer money directly, it transmits payment instructions between banks, facilitating cross-border settlements (SWIFT, 2023).

How it Facilitates Transactions

- **Standardization**: Uses ISO 20022/15022 messaging standards to ensure consistency.
- **Security**: Messages are encrypted and authenticated.
- **Connectivity**: Links over 11,000 institutions across more than 200 countries.
- **Innovation**: SWIFT Global Payments Innovation (GPI) enables real-time tracking of cross-border payments (SWIFT, 2021).

Advantages

- High **security** through encryption and authentication.
- **Global reach** ensures interoperability in international trade.
- **Efficiency** compared to manual communication.
- **Transparency** and tracking with SWIFT GPI.

Limitations

- **Costly** compared to emerging fintech solutions.
- **Intermediary banks** may delay settlement.
- **Geopolitical vulnerability**, as seen with sanctions on Russia in 2022 (European Council, 2022).
- **Cyber risks**, such as the Bangladesh Bank heist in 2016, where attackers exploited SWIFT-linked vulnerabilities (Federal Reserve Bank of New York, 2016).

Q2. Security Measures in International Banking

Critical Security Measures

- **Encryption** (AES-256, TLS 1.3) secures data in transit and storage (NIST, 2020).
- **Multi-Factor Authentication (MFA)** for user verification.
- **Intrusion detection systems (IDS/IPS)** for monitoring.
- **Secure APIs** (OAuth 2.0, OpenID Connect) for Open Banking.

- **Tokenization** replaces sensitive data like card numbers with digital tokens.

Ensuring Data Integrity & Confidentiality

- **Digital signatures & hashing** (SHA-256) ensure data is untampered.
- **Immutable audit trails** track all changes.
- **Data Loss Prevention (DLP)** protects against unauthorized exfiltration.

Regulatory Compliance

- **GDPR** (EU) and **POPIA** (South Africa) for data privacy.
- **PCI DSS** for secure card data handling.
- **FATF guidelines** for AML/CTF compliance.
- **SWIFT Customer Security Programme (CSP)** enforces mandatory cybersecurity controls (SWIFT, 2021).

Real-World Example
HSBC integrates biometric authentication and AI fraud detection to secure international payments while complying with GDPR in Europe and FATF recommendations globally (HSBC, 2022).

References (Harvard Style)

- European Council. (2022). *EU sanctions against Russia explained*. Available at: https://www.consilium.europa.eu/
- Federal Reserve Bank of New York. (2016). *Statement on Bangladesh Bank cyber incident*. New York: FRBNY.
- HSBC. (2022). *Annual Report and Accounts*. HSBC Holdings plc.
- NIST. (2020). *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology.
- SWIFT. (2021). *Customer Security Programme (CSP)*. La Hulpe: SWIFT.
- SWIFT. (2023). *About Us*. Available at: https://www.swift.com