Enterprise Technology Risk Assessment

Northbridge Digital Bank – Project 2

1. Organisation Overview

Northbridge Digital Bank is a cloud-based digital bank that provides retail and small-business banking services in the **UK, EU, and United States**. Customers use **web and mobile applications** to manage their bank accounts, make payments, and access other financial services.

Because Northbridge operates fully online, it depends heavily on **technology, cloud infrastructure, and third-party providers**. As a regulated financial institution operating in multiple regions, the bank must follow strict rules around **data protection, security, and operational resilience**.

Effective technology risk management is essential to ensure that customer data is protected, services remain available, and trust in the bank is maintained.

2. Scope of Assessment

2.1 Scope Definition

This technology risk assessment focuses on the **main systems, data, and processes** that support Northbridge Digital Bank's digital banking services.

The scope of the assessment includes:

- Core banking systems used to manage customer accounts and process transactions
- Customer-facing web and mobile banking applications
- Cloud infrastructure and identity and access management (IAM) systems
- Third-party services such as payment processors and external data providers

The assessment considers technology risks that could affect:

- **Confidentiality** – keeping customer data private
- **Integrity** – ensuring data is accurate and not altered without authorisation
- **Availability** – making sure systems remain accessible
- **Regulatory compliance** – meeting legal and regulatory requirements

3. Asset Identification and Classification

The following assets were identified as **critical** to Northbridge Digital Bank's operations. These assets are essential for delivering secure and reliable banking services and meeting regulatory obligations.

3.1 Data Assets

Northbridge Digital Bank stores and processes highly sensitive data, including:

- Customer personal data (e.g. names, addresses, dates of birth)
- Financial and transaction data related to customer accounts and payments
- Authentication and authorisation data, such as encrypted passwords and access tokens
- Regulatory, audit, and compliance records required by authorities in different regions

If these data assets were compromised, it could lead to **financial loss, regulatory fines, legal issues, and loss of customer trust**.

3.2 System Assets

The bank relies on several key systems to deliver its digital services, including:

- Core banking systems that manage accounts and transactions
- Web and mobile banking applications used by customers
- Cloud infrastructure providing computing power, storage, and networking
- Identity and access management systems that control user and administrator access
- Centralised logging and monitoring systems used to detect and respond to security incidents

Any failure or compromise of these systems could affect **service availability, data accuracy, and regulatory compliance**.

3.3 People and Process Assets

In addition to technical systems, Northbridge Digital Bank depends on people and operational processes, such as:

- Engineering, operations, and security teams responsible for building and maintaining systems
- Compliance and risk teams that ensure regulatory requirements are met
- Third-party vendors that support payments, cloud services, and data processing
- Internal processes such as incident response, change management, and access control

Weaknesses in people or processes could increase the risk of **human error, security incidents, delayed responses, or non-compliance with regulations**.

4. Threat Modelling (STRIDE)

To identify potential security threats to Northbridge Digital Bank, the **STRIDE threat modelling framework** was used. STRIDE helps categorise common security threats and ensures that risks affecting data, systems, and users are considered in a structured way.

The framework was applied to the bank's key digital assets, including customer data, cloud systems, and third-party integrations, covering both **technical and operational risks**.

4.1 Spoofing (Identity-Related Threats)

Spoofing occurs when an attacker pretends to be a legitimate user, system, or service in order to gain unauthorised access.

Possible spoofing threats at Northbridge Digital Bank include:

- Theft of customer or employee login details through phishing or social engineering attacks
- Weak authentication controls allowing attackers to log into customer accounts
- Impersonation of internal services or APIs within the cloud environment

If spoofing attacks are successful, attackers could gain access to sensitive data, perform fraudulent transactions, and damage customer trust in the bank.

4.2 Tampering (Data and System Integrity Threats)

Tampering threats involve unauthorised changes to data or systems.

Potential tampering risks include:

- Alteration of transaction data while it is being processed or transmitted
- Unauthorised changes to application code, system configurations, or cloud resources
- Modification or deletion of system logs to hide malicious activity

Tampering with critical data or systems could result in financial losses, inaccurate records, and breaches of regulatory requirements.

4.3 Repudiation (Accountability and Logging Threats)

Repudiation occurs when users or systems can deny actions because there is insufficient evidence to prove what occurred.

Key repudiation risks include:

- Incomplete or inconsistent logging of user and administrator activities
- Lack of clear audit trails for financial transactions or access events
- Limited monitoring of third-party service provider activity

Poor repudiation controls can make it difficult to investigate incidents, support regulatory audits, or assign accountability, increasing legal and compliance risks.

4.4 Information Disclosure (Confidentiality Threats)

Information disclosure threats involve unauthorised access to sensitive data.

Relevant risks include:

- Exposure of customer data due to misconfigured cloud storage or databases
- Insecure APIs leaking personal or financial information
- Excessive access permissions allowing users to view data they do not need

Information disclosure incidents may lead to regulatory penalties, reputational damage, and long-term loss of customer confidence.

4.5 Denial of Service (Availability Threats)

Denial of Service (DoS) threats aim to disrupt access to systems and services.

Potential DoS scenarios include:

- Distributed Denial of Service (DDoS) attacks targeting online banking platforms
- System outages caused by poor cloud configuration or uncontrolled resource usage
- Failures in third-party services that Northbridge depends on

Disruptions to availability could prevent customers from accessing their accounts and negatively impact the bank's operational resilience obligations.

4.6 Elevation of Privilege (Authorisation Threats)

Elevation of privilege occurs when an attacker gains higher access rights than they should have.

Key risks include:

- Misconfigured identity and access management (IAM) policies
- Users or services being granted excessive administrative permissions
- Insider misuse of privileged access

Privilege escalation could allow attackers to bypass security controls, access critical systems, and cause significant operational and security damage.

4.7 Threat Modelling Summary

The STRIDE analysis shows that Northbridge Digital Bank faces a range of **identity, data integrity, confidentiality, availability, and access control threats**. These risks are increased by the bank's reliance on **cloud infrastructure and third-party services**.

This highlights the importance of strong authentication, access controls, logging, monitoring, and governance measures to reduce the likelihood and impact of technology-related security incidents.

STRIDE Category	Threat Description	Example at Northbridge Digital Bank	Potential Impact
Spoofing	An attacker pretends to be a legitimate user or system	Phishing attack steals a customer's login details and is	Unauthorised account access, fraudulent

		used to access their account	transactions, loss of customer trust
Tampering	Unauthorised modification of data or systems	Transaction data is altered during processing or cloud configurations are changed without approval	Financial loss, inaccurate data, regulatory breaches
Repudiation	Users deny actions due to weak logging or monitoring	Lack of audit logs makes it difficult to prove who approved a high-risk transaction	Investigation difficulties, compliance issues, legal risk
Information Disclosure	Sensitive data is exposed to unauthorised parties	Misconfigured cloud storage exposes customer personal and financial data	Regulatory fines, reputational damage, loss of customer confidence
Denial of Service	Systems are made unavailable to users	DDoS attack disrupts access to online banking services	Service outages, customer dissatisfaction, operational disruption
Elevation of Privilege	An attacker gains higher access rights than intended	Misconfigured IAM policies allow a user to gain administrator access	Full system compromise, data theft, widespread operational impact

5. Risk Identification & Risk Register

5.1 Risk Assessment Methodology

Identified technology risks were assessed using a **qualitative risk assessment approach** based on:

- **Likelihood** – how likely the risk is to occur
- **Impact** – the potential effect on business operations, customers, and regulatory compliance

Risks were rated as **Low, Medium, or High**, taking into account Northbridge Digital Bank’s global operations and reliance on cloud-based systems and third-party services.

5.2 Technology Risk Register

Risk ID	Risk Name	Description	Affected Assets	Likelihood	Impact	Overall Risk Rating	Business Impact
R1	Credential Compromise via Phishing	Customer or employee credentials may be stolen through phishing or social engineering, allowing unauthorised access to banking systems	Customer data, authentication systems, core banking platforms	High	High	High	Fraudulent transactions, regulatory breaches, reputational damage
R2	Cloud Misconfiguration Data Exposure	Misconfigured cloud storage or access controls may expose sensitive customer or transaction data	Customer personal data, financial records, cloud infrastructure	Medium	High	High	Regulatory fines, breach notifications, loss of customer trust
R3	Inadequate Logging and Monitoring	Insufficient logging or monitoring may delay detection and investigation of security incidents	Logging systems, audit records, incident response processes	Medium	Medium	Medium	Increased incident impact, audit failures, regulatory scrutiny
R4	Third-Party Service Dependency Failure	Failure or compromise of third-party providers may disrupt core banking services	Payment systems, customer-facing applications, third-party integrations	Medium	High	High	Service outages, customer dissatisfaction, resilience failures
R5	Excessive Privileged Access	Poorly managed privileged	IAM systems, administrative accounts	Low–Medium	High	Medium	Large-scale data compromise,

		access may allow unauthorised privilege escalation					system disruption