1. Data Breach Risk Assessment

A multinational retail corporation experienced unauthorized access to its customer database due to a phishing attack, compromising employees' credentials and exposing sensitive personal data (PII, payment details).

1.1 Risk Identification

Element	Description
Asset at risk	Customer database containing PII and credit card data
Threat vector	Phishing attack targeting employees
Threat actor	Cyber criminals (external)
Vulnerability	Lack of phishing defense and insufficient user awareness
Business impact	Data theft, regulatory fines, reputational damage

1.2 Risk Assessment

Risk component	Assessment
Likelihood	Very likely (phishing is a frequent and effective method)
Impact	Critical (sensitive customer data exposure, fines)
Risk level	High

1.3 Mitigation Strategies

Technical Controls

- Deployed email security gateway with phishing and spoofing detection
- Implemented Multi-Factor Authentication (MFA) for internal systems
- Applied network segmentation to limit database access

Administrative Controls

- Conducted mandatory security awareness training (focus on phishing/social engineering)
- Developed and enforce a phishing response plan
- Regularly audit employee access rights and session behavior

Preventive & Detective Measures

- Used SIEM (Security Information and Event Management) for real-time alerts

- Scheduled penetration tests and vulnerability scans
- Maintained a robust incident response plan and test it regularly

Regulatory Compliance

- Ensured alignment with GDPR, CCPA, and PCI DSS
- Performed data mapping and privacy impact assessments

1.2 Summary Table

Risk	Likelihood	Impact	Risk level	Mitigation
Phishing led data breach	Very likely	Critical	High	MFA, training, SIEM segmentation, IRP

2. Regulatory Changes Risk Assessment

A financial services firm must comply with new data protection regulations issued by a government agency, requiring enhanced data privacy, encryption, and greater accountability in how customer data is handled.

2.1 Risk Identification

Element	Description
Asset at risk	Customer data and company compliance posture
Threat vector	Non compliance due to lag in adapting policies/processes
Threat actor	Government regulator, auditors
Vulnerability	Legacy systems. Poor data governance, compliance gaps
Business impact	Legal fines, reputational harm, business disruption

2.2 Risk Assessment

Risk component	Assessment
Likelihood	Likely (compliance is complex and time bound)
Impact	High (fines, operational restrictions)
Risk level	High

2.3 Mitigation Strategies

Governance Controls

- Formed a Regulatory Compliance Task Force or steering committee
- Designated a Data Protection Officer (DPO) or Compliance Lead

Policy & Procedure Enhancements

- Updated data protection policies to meet new requirements
- Created and enforce a Data Retention and Deletion policy
- Conducted Privacy Impact Assessments (PIAs) on all business processes

Technical Controls

- Encrypted all customer data at rest and in transit
- Applied Data Loss Prevention (DLP) tools
- Implemented Data Classification and Tagging

Training & Awareness

- Conducted workshops for executives and staff on new regulations
- Included compliance updates in onboarding and annual training

Monitoring & Auditing

- Regular compliance audits (internal and third-party)
- Maintained documentation for regulatory reporting and transparency

2.4 Summary Table

Risk	Likelihood	Impact	Risk level	Mitigation
Failure to meet new regulatory standards	Likely	High	High	DPO, audits, encryption, PIA, polcy updates

Conclusion and Recommendations

Both scenarios present high-risk profiles with regulatory and operational implications. The organization should:

- Address the data breach threat immediately through layered security, user education, and real-time monitoring.
- Proactively align with regulatory changes by strengthening data governance and embedding compliance into business practices.