**Unit 6 Seminar - Security Standards**

## 1. Applicable Security Standards

For this exercise, let's consider a **large international bank based in the UK** (from a previous assessment):

- **General Data Protection Regulation (GDPR):**
  Since the organisation operates in the UK and processes personal data of EU and UK citizens, GDPR compliance is mandatory. GDPR ensures the protection of personal data and imposes strict rules on data processing, storage, and transfer.
- **Payment Card Industry Data Security Standard (PCI-DSS):**
  As a bank handling online payments and transactions, compliance with PCI-DSS is essential to safeguard payment card information.
- **Health Insurance Portability and Accountability Act (HIPAA):**
  HIPAA is unlikely to apply to this organisation unless it processes or stores protected health information (PHI). This standard primarily concerns organisations operating in the healthcare sector.

## 2. Evaluating the Organisation Against Standards

### GDPR

**Key Requirements:**

1. **Lawfulness, Fairness, and Transparency:** The bank must process data based on lawful grounds and provide clear privacy notices.
2. **Data Minimisation and Accuracy:** Only necessary personal data should be collected and kept up-to-date.
3. **Accountability:** Demonstrate compliance through records of processing activities and data protection impact assessments (DPIAs).

**Evaluation Process:**

- Conduct an internal audit of data processing activities to ensure they align with GDPR principles.
- Review privacy policies, consent mechanisms, and data retention schedules.

- Assess security measures like encryption and access controls for protecting personal data.

**PCI-DSS**

**Key Requirements:**

1. **Maintain a Secure Network:** Use firewalls and avoid vendor-supplied defaults for system passwords.
2. **Protect Cardholder Data:** Encrypt cardholder data at rest and during transmission.
3. **Monitor and Test Networks:** Regularly test systems and monitor access logs.

**Evaluation Process:**

- Perform vulnerability scans and penetration tests to identify gaps in the bank's payment systems.
- Verify encryption protocols for data in transit and at rest.
- Check compliance with multi-factor authentication (MFA) for accessing payment systems.

**3. Recommendations to Meet Standards**

**To Meet GDPR Requirements:**

1. **Appoint a Data Protection Officer (DPO):** Responsible for overseeing compliance and acting as the point of contact for regulators.
2. **Implement Data Privacy by Design:** Ensure all systems are designed with data protection principles from the outset.
3. **Enhance Transparency:** Update privacy policies, this policy should outline the organisation's approach to data security, employee responsibilities. and ensure clear communication with customers regarding their rights.
4. **Conduct Regular DPIAs:** Identify risks associated with new data processing activities and implement mitigations.
5. Train employees on data security: Employees should be aware of the organisation's security policies and procedures, and how to identify and report security risks.

6. Regularly monitor and review security controls: This ensures the effectiveness of security measures and identifies areas for improvement.

**To Meet PCI-DSS Requirements:**

1. **Strengthen Payment Systems Security:** Use tokenisation and encryption to secure payment data.
2. **Access Control Measures:** Implement role-based access controls (RBAC) to limit access to sensitive data.
3. **Conduct Regular Audits:** Schedule quarterly vulnerability scans and annual PCI assessments by a Qualified Security Assessor (QSA).
4. **Employee Training:** Educate employees on handling cardholder data securely and recognising phishing attempts.

**4. Assumptions Made**

1. **GDPR Applicability:** The organisation processes data of EU/UK citizens, which necessitates compliance with GDPR.
2. **PCI-DSS Applicability:** The organisation handles online payments, requiring compliance with PCI-DSS.
3. **HIPAA Exclusion:** The bank does not process health-related data, making HIPAA irrelevant.
4. **Current Security Posture:** The bank already has some security measures in place, such as firewalls and encryption, but gaps may exist in meeting specific standards.

**Conclusion**

This organisation must prioritise compliance with GDPR and PCI-DSS to ensure the protection of personal and financial data. Regular audits, employee training, and robust technical controls are critical steps toward achieving compliance. By adhering to these standards, the bank can mitigate security risks, maintain customer trust, and avoid regulatory penalties.

**References**


- ICO (2020). *Guide to the General Data Protection Regulation (GDPR).* Available at: https://ico.org.uk

- PCI Security Standards Council (2020). *PCI Security Standards Overview.* Available at: https://www.pcisecuritystandards.org
- HIPAA Guide (2020). *HIPAA For Dummies.* Available at: https://www.hipaaguide.net