WEEK 2 SCENARIO-BASED ASSIGNMENT

Student Name: Oluwatimilehin Oluwagbemi

Reg. No: 2025/GRC/10712

Date: 02/08/2025

Scenario 1: Global E-commerce Platform

Executive Summary:

TechMart Global's data handling and customer reach present multi-regulatory compliance challenges. The GDPR, CCPA, PIPEDA, and Australia's Privacy Act are among the important laws from various jurisdictions that are identified in this analysis.
The suggested action plan ensures that the business complies with international privacy standards and protects customer trust by offering both short-term and long-term recommendations along with cost estimates.
1.1 Regulatory Identification:

The identified applicable regulations are:

- The European Union's General Data Protection Regulation (GDPR): is applicable since it is a fundamental data privacy law with an international scope. The use of cookies and tracking technologies for website optimization, the expansion of operations to serve customers in the EU, and the processing of personal data, including name, address, and payment information of EU customers, are the triggers for this compliance.
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), also known as the Privacy and Electronic Communications Regulations (PECR). The UK GDPR is supplemented by the DPA 2018, and cookies and electronic marketing are covered by PECR. Personalized marketing, which is covered by PECR, the use of cookies and tracking technologies, and the gathering and processing of customers in the UK are the triggers for this compliance.
- Personal Information Protection and Electronic Documents Act (PIPEDA) – Canada: Canada’s Federal law appliable to private sector which applies to organizations that collect, use or disclose personal information in the course of commercial activities across Canada. The triggers for this compliance include; TechMart’s commercial activity, collection of customer’s data.

- Privacy Act 1988 (including Australian Privacy Principles - APPs) – Australia: this law is Australia’s primary privacy law which regulates how Australian Government agencies and most private sector organizations must handle personal information, which is applicable to TechMart given its global scale. The triggers for this compliance include; processing of personal information of customers in Australia.

- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) - United States (California Specific): the United States does have some influential

state-level laws such as the CCPA and CPRA that applies to organizations meeting specific thresholds that collect, use, or sell personal information of California residents. The triggers for this compliance include; sharing of customer's analytic with third-party marketing partners which is a key factor as this constitutes a sale or sharing of data in the CCPA/CPRA law.

- Personal Data Protection Act (PDPA) – Singapore: TechMart explicitly stores customer data on servers located in Singapore, this law applies to TechMart, because, the act of storing and processing data within Singapore's border brings them under the purview of PDPA. The triggers for this compliance include; storing of customer data on servers located in Singapore, regardless of the nationality or location of the data subject.

- Digital Personal Data Protection Act, 2023 (DPDP Act) – India**:** this applies to TechMart because it processes customer's interaction through a call center in India, the trigger for this compliance include; the existence of a call center in India implies that personal data is being accessed, processed, and potentially stored by individuals and systems located in India.

1.2 GDPR Compliance Assessment:

Legal Basis for Processing Customer Data: under GDPR, every processing activity must have a lawful basis as outlined in Article 6. TechMart processes a variety of customer data for different purposes such as:

- Names, Addresses, Payment information which falls under the contractual necessity in Article 6(1)(b) of the GDPR, TechMart must ensure that only data strictly necessary for contract performance is collected under this basis.
- Browsing history, sharing of customer's analytics to third-party: this legal basis combines consent under Article 6(1)(a) and legitimate interest under Article 6(1)(f). TechMart must ensure users have a clear opt-in mechanism especially involving use of cookies and tracking technologies, they must adopt data minimization and data storage principles.

Data subject rights implementation requirements: TechMart must have robust mechanisms to facilitate individual several rights granted by GDPR (Articles 12-22), such as; right to be informe- (Articles 13&14), right of access-(Article 15), right to rectification-(Article 16), right to erasure/forgotten-(Article 17), right to restriction of processing-(Article 18), right to data portability-(Article 20), right to object-(Article 21), and rights related to automated decision making and profiling-(Article 22).

International data transfer compliance: chapter 5 of the GDPR strictly govern transfers of data to other countries. TechMart would need to self-certify under DPF to lawfully transfer EU data to its US operations. TechMart must implement SCCs with the entity operating the Singapore servers, along with a robust TIA-(Transfer-Impact-Assessment) and potentially supplementary measures. TechMart must implement SCCs with the Indian call center as a data processor, and conduct a TIA. The absence of clear documentation on transfer mechanisms and TIAs represents a significant gap.

Potential compliance gaps and risks: the following are the compliance gaps and risks associated to TechMart under GDPR:

- Lack of valid legal basis for marketing/profiling: TechMark lack explicit consent for personalized marketing, recommendation of algorithms, and non-essential cookie/tracking. For illegal processing, they face high risk or regulatory penalties, especially under Article 6 and the ePrivacy Directive.
- Indefinite Data Retention: TechMart violates both the right to erasure (Article 17) and the storage limitation principle (Article 5(1)(e)) by keeping customer data indefinitely for business intelligence purposes. Therefore, they are subjected to Significant fines, data breach exposure (more data for longer means higher risk), and inability to comply with erasure requests.
- Non-Compliant International Data Transfers: TechMart lack documentation and proper implementation transfer mechanisms for data flowing to the US, Singapore, and India, as well as to third-party marketing partners. Therefore, they are subjected to Severe fines (e.g., up to 4% of global annual turnover or €20 million, whichever is higher). This is one of the highest risk areas.
- Data Minimization & Purpose Limitation: TechMart collects Browse history, and purchase patterns and retains data indefinitely without clear justification for *each* data point and *each* purpose. Over-collection of data increases compliance burden and risk in case of a breach, violates Article 5(1)(c) and (b).
- Third-Party Vendor Management: TechMart sharing customer analytics with third-party marketing partners likely requires formal Data Processing Agreements (DPAs) under Article 28, ensuring these partners also comply with GDPR. Therefore, they are subjected to Joint liability for non-compliance by partners, and potential fines if DPAs are absent or inadequate.

1.3 Compliance Recommendations:

Immediate Actions required (0-30 days): TechMart must perform a comprehensive GDPR audit, designate a Data Protection Officer (DPO), update their cookie and privacy banners to comply with the GDPR and ePrivacy, implement data minimization, terminate indefinite retention, and establish a legitimate basis for all processing operations.

Short-Term Improvements (1-6 Months): TechMart should implement SCCs for data transfers, develop workflows for handling DSARs, educate employees about data rights and laws, adjust website analytics to respect user consents, and introduce an automated consent management system.

Long-Term Strategy (6-12 Months): TechMart should implement privacy framework like ISO/IEC 27701, incorporate privacy-by-design principles into the architecture of the website, check vendor contracts for legal provisions, and investigate third-party certification to ensure privacy.

Estimated Costs and resource requirements:

Item	Estimated costs	Resource requirement
DPO Hiring	$500-$10,000/month	Legal, HR
Consent Management	$15,000 plus	IT, Legal
Training $ Awareness	$2,000-$5000	HR, Communications
Compliance Audit	$10,000	Consultants

Scenario 2: Healthcare Technology Startup

Executive Summary:

MedConnect, a U.S.-based healthcare tech startup with plans to go global, uses cloud systems, AI, and mobile apps to handle sensitive health data. This response examines state-level privacy laws, relevant regulations like HIPAA, and international data protection frameworks like PIPEDA and GDPR. A comprehensive data security assessment identifies business associate responsibilities and emphasizes technical, administrative, and physical safeguards. A responsive breach plan is prompted by the company's recent security incident.

2.1 Regulatory Framework Analysis:

HIPAA Requirements and Applicability: MedConnect is designated as a Business Associate because it generates, receives, maintains, and transmits PHI on behalf of Covered Entities. The privacy rule, which regulates the use and disclosure of PHI and guarantees patients' control over their health information, is one of the main requirements that are triggered. MedConnect must make sure that it only uses and discloses PHI in accordance with HIPAA.

State-level healthcare privacy laws: Many US states have passed their own privacy laws, which may be stricter or more comprehensive than HIPAA, even though it offers a federal floor. This is relevant to MedConnect because it has to abide by state laws in each of the ten states where it conducts business.

International regulations for planned expansion: MedConnect's planned expansion to Canada and the European Union introduces significant new regulatory obligations. The regulatory obligations include:

- European Union (EU) - General Data Protection Regulation (GDPR) and European Health Data Space (EHDS): GDPR applies due to MedConnect extra-territorial reach (Article 3) by processing personal data of individuals located in the EU.
- Canada - Personal Information Protection and Electronic Documents Act (PIPEDA) and Provincial Health Privacy Laws: PIPEDA is Canada's federal private sector privacy law. It applies to organizations collecting, using, or disclosing personal information in the course of commercial activities of or in addition to PIPEDA, particularly for health information custodians.

Industry-specific compliance considerations: healthcare industry has unique compliance challenges beyond the general data privacy laws especially with the use of emerging technologies like AI. MedConnect's AI for personalized health recommendations might fall

under these emerging regulations, requiring rigorous testing, validation, and ongoing monitoring.

2.2 Data Security and Privacy Assessment:

Technical safeguards required under HIPAA Security Rule: The HIPAA Security Rule mandates specific technical safeguards to protect Electronic Protected Health Information (ePHI). MedConnect, using a mobile app and cloud servers, must implement these vigorously. The safeguards include:

- Access control: MedConnect must ensure unique user IDs for patients and healthcare providers.
- Audit control: MedConnect needs comprehensive audit logging for all access to medical records, communications, and system configurations.
- Person or Entity Authentication: Beyond passwords, MedConnect should implement strong authentication, such as multi-factor authentication (MFA).

Administrative and Physical safeguards implementation: represents the policies, procedures and management, which are the cornerstone of a strong security programs. Some administrative safeguards and physical safeguards are listed below:

- Security management process: MedConnect must conduct thorough and regular HIPAA-compliant risk assessments.
- Assigned security responsibility: there must be as designated security official who oversees security operations of the organization.
- Security awareness and training: MedConnect must implement mandatory security and privacy awareness training for all staff, especially those handling PHI or supporting the platform. This training should cover phishing, malware, secure password practices, and incident reporting.
- Contingency Plan: MedConnect's reliance on cloud servers means they need to ensure the CSP's contingency plans align with HIPAA requirements
- Workstation use and security: policies must be in place for workstation usage and physical safeguards for workstations accessing ePHI.

Business Associate Agreement Requirements: MedConnect *must* have a HIPAA-compliant BAA in place with each of its 50 healthcare provider partners *before* receiving or processing any PHI from them. MedConnect *must* also have a HIPAA-compliant BAA with its major cloud service provider.

Breach Notification obligations and procedures: MedConnect, as a BA, must notify the affected Covered Entities (healthcare providers) **without unreasonable delay and in no case later than 60 calendar days** after discovery of the breach.

2.3 Incident Response and Remediation:

Immediate containment and assessment steps: upon detection of any security incident, MedConnect must act swiftly to contain the breach and gather critical information, they must activate incident response team (IRT), isolate and contain the breach, preserve evidence and perform initial risk assessment.

Regulatory notification requirements and timelines: MedConnect must adhere to strict breach notification timelines and requirements across applicable jurisdictions, such as the United States HIPAA Breach Notification Rule, European Union – GDPR and Canada PIPEDA.

Patient communication strategy: there must be a transparent communication strategy for patients, in a case of security breach, the breach must be communicated to them in a clear, and easy-to-understand manner, describing what happened including the date the breach occurred, the data that was compromised, steps taken by MedConnect to contain the breach, the steps they can take to protect themselves going forward, the communication must be passed across through proper channels.

Long-term security improvements to prevent future incidents: MedConnect must conduct a thorough internal and external investigations to know the root cause of the incident, analyze the effectiveness of the incident response plan and identify areas for improvement, they must document all findings, corrective actions taken, lessons learned.

Scenario 3: Financial Services Firm

Executive Summary:

SecureBank, a mid-sized financial services provider, faces multi-regulatory pressures due to its handling of sensitive payment and financial data, mounting cybersecurity risks, and customer trust challenges. This report outlines a comprehensive strategy for PCI DSS implementation and presents a unified compliance approach that balances innovation with risk management. A robust framework for continuous improvement is proposed, encompassing vendor oversight, staff training, and incident planning, to strengthen security posture and meet regulatory expectations.

3.1 Multi-Regulatory Compliance Analysis:

PCI-DSS requirements for payment card data: As a firm processing over 6 million transactions annually, SecureBank is a **Level 1 Merchant**, requiring the highest level of validation (annual Report on Compliance by a Qualified Security Assessor (QSA)). This is triggered by the acceptance/processing of payment cards, volume of transactions and storage of cardholder data.

Banking regulations for financial data protection: Financial institutions in the U.S. are subject to a robust set of federal and state laws and regulations designed to protect consumer financial privacy and ensure the security of financial data such as:

- Gramm-Leach-Bliley Act (GLBA)
- Federal Trade Commission (FTC) Act Section 5
- Bank Secrecy Act (BSA)/Anti-Money Laundering (AML)

- Right to Financial Privacy Act (RFPA) and
- State Banking Laws.

Consumer protection laws for financial services: such as Dodd-Frank Wall Street Reform and Consumer Protection Act (specifically, the Consumer Financial Protection Act of 2010), Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA), and, Electronic Funds Transfer Act (EFTA) / Regulation E.

Cross-regulatory compliance challenges and solutions: challenges faced include; overlapping and potentially conflicting requirements, dynamic regulatory landscape, resource intensiveness, third-party risk management and audit fatigue. Solutions to address these challenges include; integrated GRC program, dedicated compliance team and expertise, technology investment, robust vendor management program, regular training and awareness, and proactive regulatory monitoring.

3.2 PCI-DSS Implementation plan

The 12 PCI-DSS requirements and their application, SecureBank should:

- Review and optimize their firewall configurations, intrusion detection/prevention system and network segmentation.
- Address legacy systems by either upgrading them to support secure configurations or isolate them tightly within network segments
- Implement strong encryption for PAN at rest, implement tokenization for recurring transactions to minimize stored PAN exposure.
- Secure online banking and mobile app communications, ensure all third-party integrations such as payment processors or credit bureaus use strong and modern encryption protocols.
- Implement advanced endpoint protection (EDR) across all devices and servers, regularly update signatures and ensure centralized monitoring.
- Implement a robust patch management program.
- Define granular roles and permissions for employees across all departments accessing sensitive financial data.
- Secure data centers, manage physical access to servers, network devices, and document storage.
- Implement a comprehensive Security Information and Event Management (SIEM) system to centralize logs from all platforms.
- Beyond quarterly ASV scans, conduct internal vulnerability scans monthly/quarterly. Perform annual penetration tests.
- Develop comprehensive, documented security policies and procedures.

Compliance level determination and validation process: SecureBank qualifies as a **Level 1 Merchant**. Validation process for level 1 merchant include:

- Annual report on compliance (ROC)
- Quarterly external vulnerability scans
- Annual attestation of compliance (AOC)
- Continuous compliance.

Technical and procedural controls implementation:

Technical controls:

- Encryption and tokenization
- Network security
- Access management
- Logging and monitoring
- Vulnerability management

Procedural controls:

- Define roles and responsibilities.
- Policy and procedure documentation.
- Change management.
- Employee training.
- Third-party due diligence.

Ongoing Monitoring and maintenance requirements:

- Continuous Monitoring
- Regular reviews of all PCI-DSS controls, policies and procedures
- Annual reassessment
- Incident response integration

3.3 Risk Management and Continuous Improvement:

Regular compliance assessments and gap analysis:

- Perform annual formal compliance audits
- Continuous monitoring and data mapping
- Report gap analysis
- Perform control effectiveness testing
- Monitor regulatory change

Vendor management and third-party risk assessment: Before engaging a third-party vendor, conduct a thorough due diligence that include security assessment, risk assessment and contractual requirement. Execute comprehensive Service Level Agreements (SLAs) and Data Processing Agreements (DPAs) that clearly define roles, responsibilities, security requirements, and breach notification obligations.

Employee training and awareness programs: Human error is a leading cause of breaches, SecureBank should develop and deliver comprehensive, mandatory security and privacy awareness training for *all* employees.

Incident response and business continuity planning:

- Incident response plan (IRP): this must contain phases that addresses detection & analysis, containment, eradication, recovery and post-incident activity.
- Business continuity plan (BCP): Create and regularly update BCP documents to ensure critical business functions can continue or quickly resume operations after a disruption.

Scenario 4: International Manufacturing Corporation

Executive Summary:

International Manufacturing Corporation, faces fragmented compliance obligations across jurisdictions and the growing threat of industrial espionage. This analysis recommends an integrated implementation of ISO standards (27001, 27701, 31000) to unify compliance efforts.

4.1 ISO Standards Integration Strategy:

ISO/IEC 27001 for information security management: this will ensure confidentiality, integrity, and availability of information.

ISO/IEC 31000 for risk management: this identifies, evaluates, and mitigates risks across all operation, not just information security risk.

ISO/IEC 27701 for privacy information management: this is an extension of ISO 27001 which address potential data protection requirements aligned with GDPR and other laws.

Integration approach and implementation timeline:

Integration Approach:

- ISO 27001 will serve as the overarching framework. All information security controls, policies, procedures, risk assessments, and incident management processes will be built around ISO 27001's requirements.
- ISO 31000 for Enhanced Risk Management. It will inform and strengthen the risk assessment and risk treatment processes within the ISO 27001 ISMS. This ensures that International Manufacturing Corporation approach to identifying, analyzing, evaluating, and treating information security risks is robust, consistent, and aligned with enterprise-wide risk management principles.
- **ISO 27701 for Privacy Extension:** Once the ISO 27001 ISMS is being established, ISO 27701 can be integrated as an extension to specifically address privacy information management. Such as mapping PII and privacy controls.

Estimated timeline:

- Phase 1: Planning & ISO 27001 ISMS Foundation (6-9 months)

- Phase 2: ISO 27001 Certification & ISO 27701 Integration (3-6 months after Phase 1)
- Phase 3**:** ISO 27701 Certification & Continuous Improvement (3-6 months after Phase 2)

Benefits and challenges of multi-standard certification:

Benefits:

- Unified security and privacy posture
- Demonstrated commitment and trust
- Competitive advantage
- Enhanced risk management
- Streamlined compliance

Challenges:

- Resource intensiveness
- Complexity and scope management
- Cultural resistance
- Maintaining momentum
- Lack of qualified personnel/consultants.

4.2 Cross-Jurisdictional Compliance Framework

Regulatory variations across different countries and regions:

Europe (EU): International Manufacturing Corporation must comply with GDPR

North America: International Manufacturing Corporation must comply with state privacy laws such as California Consumer Privacy Act/CPRA and others.

Canada: International Manufacturing Corporation must comply with Personal Information Protection and Electronic Documents Act (PIPEDA)

Asia: International Manufacturing Corporation must comply with China: Personal Information Protection Law (PIPL), Japan: Act on Protection of Personal Information (APPI), Singapore: Personal Data Protection Act (PDPA), India: Digital Personal Data Protection Act (DPDP Act), and South Korea: Personal Information Protection Act (PIPA).

Harmonization strategies for conflicting requirements: International Manufacturing Corporation should adopt a highest common denominator approach. International Manufacturing Corporation can:

- Adopt a GDPR-Plus or PIPL-Plus Baseline.
- **Focus on Core Privacy Principles**
- **Implement Centralized Risk Assessment & Treatment**
- **Implement International Data Transfer Mechanisms**

- **Implement Privacy by Design and Security by Design**.

Unified policies and procedures that meet multiple regulatory standards:

- Global Information Security Policy
- Global Data Protection and Privacy Policy
- Standard Operating Procedures (SOPs)

Governance structure for ongoing compliance management: A robust governance structure ensures accountability, oversight, and continuous improvement such as:

- Executive Leadership & Oversight
- Global GRC (Governance, Risk, and Compliance) Committee
- Regional/Local Compliance Leads/Data Protection Officers (DPOs)
- Centralized GRC Platform

4.3 Emerging Technology Risk Assessment

IoT devices and data collection considerations: IoT devices in manufacturing collect vast amounts of data, including operational data, performance metrics, and potentially personal data. The sheer volume and real-time nature of IoT data can overwhelm traditional security and compliance monitoring systems.

Industry 4.0 and operational technology security: Industry 4.0 involves the convergence of IT and OT bringing real-time data from the factory floor into IT systems for analysis and control. This blurs traditional security boundaries, expanded attack surface, increase physical security risks, impacted legacy system vulnerabilities.

Data sovereignty and cross-border data transfer issues: With operations in North America, Europe, and Asia, International Manufacturing Corporation might face complex data sovereignty requirements, which dictate that data is subject to the laws of the country where it is collected or stored, such as Data Localization, Cross-Border Transfer Mechanism and Non-Personal Data Sovereignty.

Future regulatory trends and preparation strategies: The regulatory landscape for digital technologies is rapidly evolving, demanding continuous adaptation, there will be:

- Increased Focus on AI Governance and Ethics
- Supply Chain Security Mandates
- Threat Intelligence Sharing: Establish formal processes for receiving and acting upon threat intelligence.
- Mandatory Security Certifications
- Digital Operational Resilience (DORA - EU Financial Services)

References:

https://gdpr-info.eu/art-3-gdpr/

https://gdpr.eu/article-3-requirements-of-handling-personal-data-of-subjects-in-the-union/

https://www.itgovernance.co.uk/data-protection

https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html#h-416888

https://www.oaic.gov.au/privacy/australian-privacy-principles

https://www.cookiebot.com/en/cpra/

https://sso.agc.gov.sg/Act/PDPA2012

https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Act,_2023

https://www.dlapiperdataprotection.com/?t=law&c=IN

https://gdpr-info.eu/art-6-gdpr/

https://gdpr-info.eu/art-12-gdpr/

https://gdpr-info.eu/art-13-gdpr/

https://gdpr-info.eu/art-14-gdpr/

https://gdpr-info.eu/art-15-gdpr/

https://gdpr-info.eu/art-16-gdpr/

https://gdpr-info.eu/art-17-gdpr/

https://gdpr-info.eu/art-18-gdpr/

https://gdpr-info.eu/art-19-gdpr/

https://gdpr-info.eu/art-20-gdpr/

https://gdpr-info.eu/art-21-gdpr/

https://gdpr-info.eu/art-22-gdpr/

https://gdpr-info.eu/art-5-gdpr/

https://gdpr-info.eu/art-28-gdpr/

https://www.dataprivacyframework.gov/Program-Overview

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

https://en.wikipedia.org/wiki/Financial_privacy_laws_in_the_United_States#:~:text=In%20the%20United%20States%2C%20financial,the%20Fair%20Credit%20Reporting%20Act.