# WEEK 4 SCENARIO-BASED ASSIGNMENT

Student Name

Oluwatimilehin Oluwagbemi

Reg. No

2025/GRC/10712

Date

14th August, 2025

Course Title

GRC 101 – Introduction to Governance, Risks and Compliance

EXECUTIVE SUMMARY

TechFlow, a rapid growing financial technology company, faces a severe compliance crisis as a result of its rapid growth outpacing its regulatory infrastructure. FinCEN and the PCI SSC have discovered significant flaws as a result, which have resulted in losses exceeding $5 million and jeopardized the company's planned initial public offering (IPO).

The major issues identified include:

- Weak Governance: No dedicated Chief Compliance Officer (CCO) or compliance committee.
- Outdated Policies: Inconsistent and missing policies, especially for new business lines.
- Inadequate Training: Ad-hoc and untracked compliance training.
- Lack of Monitoring**:** Reactive approach to compliance issues with no systematic oversight.
- Poor Documentation**:** Inconsistent, manual, and error-prone record-keeping.
- Legacy Technology**:** Reliance on outdated systems with limited compliance capabilities.
- Insufficient Third-Party Oversight: Poor management of vendor compliance.

To address these issues, a comprehensive transformation design has been proposed, focusing on a phased integrated approach stated below:

- Making compliance a core business function or operation is the aim of a compliance program. This design includes the appointment of a chief compliance officer (CCO) who will report directly to the Board compliance committee, as well as a dedicated compliance department with specialized teams like AML, PCI DSS, Data Security, Regulatory & Enterprise Compliance, and compliance liaisons embedded within business units. A formal governance framework and transparent accountability protocols, including an anonymous whistleblower mechanism, will be implemented.
- A policy and procedure were created with the intention of substituting a structured policy framework for the inconsistent practices. This will standardize policy templates, create a tiered policy hierarchy and classification system, and put in place a strong lifecycle management procedure for the creation, approval, and routine review of policies. Every policy, accompanied by a formal communication and a required role-specific training plan, will be kept in a single digital repository.
- A risk assessment and monitoring plan is developed in order to shift TechFlow's risk management strategy from reactive to proactive. With an emphasis on AML, PCI DSS, and third-party risks, this means implementing a systematic framework to identify, assess, and mitigate compliance risks in all operations. This plan will also incorporate automated monitoring, frequent reviews, explicit escalation protocols for compliance issues, and independent testing (internal and external audits).
- The primary objective of the documentation and reporting system is to provide a centralized, digital system for accurate data and actionable insights. Important first steps include a comprehensive framework of Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs), a secure Document Management System (DMS) with version control and audit trails, and standardized reporting templates for the Board of Directors, Executive Management, and Business Units.
- Implementation Roadmap is designed which will be executed in three phases over 12 months. Phase 1 (0-3 months) will meet immediate regulatory demands and mitigate

critical risks, a CCO will be appointed, rapid risk assessment will be conducted, core policies will be updated, there will be an initial training and remediation plan will be submitted. The estimated cost for phase 1 ranges from $500,000 - $1,000,000. Phase 2 (4-9 months) compliance framework will be expanded, and technology will be integrated, comprehensive policy framework will be developed, GRC platform will be implemented, advanced monitoring will be conducted and third-party risks will be managed. Phase 3 (10-12 months) this phase will refine processes and embed a strong compliance structure with an annual program review, analytics optimisation, and preparation for future regulatory cycles. Annual estimated cost for this phase ranges from $1.75 million to $4.85 million (excluding the one-time GRC costs of $200k - $700k).

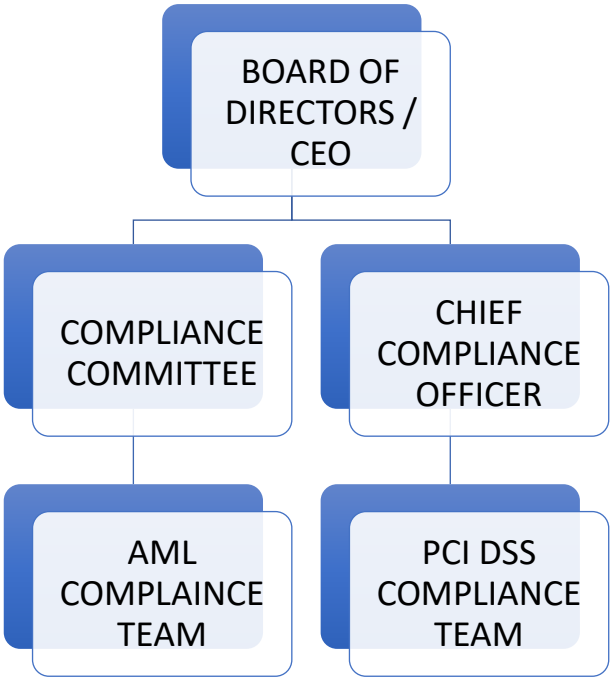
Strong leadership support, open communication regarding the change's justification, focused training, and employee feedback systems are all necessary for the successful execution of this comprehensive transformation design. This thorough plan is essential to TechFlow's long-term survival, standing, and development. Its goals are to end the current crisis, win over stakeholders, and clear the path for future growth and an IPO.

## TASK 1 - COMPLIANCE PROGRAM DESIGN

By building a robust and long-lasting compliance management system for TechFlow Industries, the goal is to address the identified flaws and meet regulatory requirements. This design will be based on the seven elements of a successful compliance program as stated in Chapter 8 of the U.S. Sentencing Guidelines. These elements ensure that a company not only prevents and detects misconduct, but also cultivates an ethical culture. The scope of this program encompasses the business units, subsidiaries, and third-party relationships of all TechFlow industries in all three of its geographic locations (the United States, Canada, and Mexico). It will specifically address general regulatory compliance that pertains to a financial technology company handling sensitive financial data, financial crime prevention (AML, Sanctions), and data security (PCI DSS). The objectives are to:

- establish mechanisms for the proactive prevention, detection, and prompt resolution of legal, regulatory, and internal policy violations, particularly those related to AML and PCI DSS;
- ensure that all applicable federal, state, and international financial regulations, such as PCI DSS and the FinCEN AML program's requirements are fully followed;
- foster a strong culture of compliance and ethics throughout the entire organization, from the Board of Directors to individual employees;
- assess, identify, and minimize compliance risks in all business operations; integrate compliance practices into daily operations to boost output and minimize disruptions; and shift from a reactive to a proactive compliance posture.;
- regain and maintain the trust of banking partners, staff, investors, and customers by demonstrating a commitment to strict compliance;
- build a scalable compliance framework that can adapt to TechFlow's continued growth and expansion into new markets and services.

Organizational Chart showing compliance structure:



**TECHFLOW INDUSTRIES COMPLIANCE PROGRAM CHARTER**

Purpose and Authority:

This Charter sets out the goals, powers, and parameters of TechFlow Industries' (the "Company") Compliance Program. The Compliance Program is intended to prevent, identify, and address infractions of relevant laws, rules, and internal policies, especially those pertaining to finance industry data security standard (PCI DSS) requirements, anti-money laundering (AML) as required by FinCEN, and other financial regulations. The Board of Directors has direct authority over the establishment of this program.

Scope:

The Compliance Program is applicable to TechFlow Industries' worldwide operations, business divisions, subsidiaries, workers (including contract and temporary workers), and third-party suppliers. It includes all of the goods, services, and transactions that the business handles. Specific areas of focus include, but are not limited to:

- Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF)
- Sanctions Compliance
- Payment Card Industry Data Security Standard (PCI DSS)
- Data Privacy and Security (e.g., consumer data protection)
- Consumer Protection Regulations
- Anti-Bribery and Corruption
- Fraud Prevention
- Regulatory Reporting and Filings

Objectives:

The primary objectives of the Compliance Program are to:

- Ensure TechFlow Industries full adherence to all applicable laws, regulations, and industry standards, including FinCEN AML Program Requirements and PCI DSS
- Identify, assess, and mitigate compliance risks across all business activities.
- Establish and maintain effective internal controls to prevent and detect compliance failures.
- Foster a strong, ethical culture where compliance is embedded in all business decisions and operations.
- Provide robust training and communication to ensure all employees understand their compliance obligations.
- Establish clear reporting mechanisms for compliance concerns and enable prompt, effective remediation of identified issues.
- Protect the company’s reputation, financial stability, and operational licenses.
- Support sustainable business growth by integrating compliance seamlessly into expansion strategies.

Governance and Oversight

a. Board of Directors: board of directors hold ultimate responsibility for the oversight of the compliance program, they must ensure the program receives adequate resources and support to operate effectively and independently. The board will receive regular reports on the program's effectiveness, significant risks, and any material compliance incidents.
b. Compliance Committee: a dedicated compliance committee will be established; the committee will include independent directors. This committee will oversee the design, implementation, and effectiveness of the Compliance Program; review and approve the Compliance Program charter, key compliance policies, and procedures; monitor significant compliance risks and track remediation efforts for identified deficiencies; ensure the chief compliance officer (CCO) has direct access to the Board and operates with sufficient authority and independence; review internal and external audit findings related to compliance; approve the annual compliance plan and budget; meet at least quarterly, or more frequently as needed.
c. Chief Compliance Officer (CCO): CCO will be appointed as an executive-level position, reporting directly to the compliance committee and administratively to the CEO. The CCO will be responsible for the day-to-day management and execution of the compliance program. The CCO will have sufficient authority and independence to discharge their duties effectively; direct access to all business units, employees, and relevant information; adequate resources (staff, technology, budget) to fulfil responsibilities; responsibility for reporting significant compliance matters to the compliance committee and senior management.

Program Elements

The Compliance Program will be structured around the seven elements of an effective compliance program following the U.S. Sentencing Guidelines, Chapter 8:

1. Standards and procedures: standards and procedures will be established to prevent and detect criminal conduct. Code of conduct that addresses areas of potential criminal liability will be written, there will be specific policies and procedures for high-risk areas, clear standards will be set for personnel behaviour and regular updates to reflect changes in law and business operations will be conducted.
2. High-Level Personnel Responsibility: Board of Directors, Chief Compliance Officer must have sufficient authority and resources to implement the compliance program effectively, they must also demonstrate commitment to compliance and ethics.
3. Due Care in Delegation: this requires ongoing vigilance, there must be a system that detects misconduct by personnel in positions of authority, and appropriate actions should be taken if such misconduct is discovered.
4. Communication and Training: this must be practical and tailored to employee's role and responsibilities, it must be continuous and updated regularly.
5. Monitoring and Auditing: monitoring must be risk-based, and must cover all significant areas of potential criminal liability, TechFlow must have systems to detect violations before they are reported by external sources. Auditing must be independent and objective.
6. Incentives and Disciplinary Measures: disciplinary measures must be applied consistently regardless of the position or status of the individual involved. There must

be clear procedure for investigating allegations and must protect employees who report violations in good faith.

7. Response and Prevention: response must be proportionate to the violation and must address underlying causes, not just symptoms.

Reporting and Accountability

- Internal reporting: there must be clear channels for employees to report compliance concerns including an anonymous whistleblower hotline, without fear of retaliation.
- External reporting: there must be compliance with all regulatory reporting obligations such as SARs to FinCEN.
- Accountability: all employees, from board level to entry-level staff, are accountable for adhering to compliance standards. Compliance performance will be a factor in performance evaluations and compensation decisions. Disciplinary actions for violations should be consistently applied.

Review and Amendment

This charter should be reviewed at least annually by the Compliance Committee and approved by the Board of Directors to ensure its continued relevance and effectiveness. Any material amendments to this Charter must be approved by the Board of Directors.

**ROLE DESCRIPTIONS FOR KEY COMPLIANCE POSITIONS**

a. Chief Compliance Officer (CCO): reports to Compliance Committee directly and CEO administratively. Key responsibilities of a CCO include:

    i. Designs, implements, and oversees the overall compliance program.
    ii. Develops and maintains compliance policies, procedures, and controls.
    iii. Identifies, assesses, and monitors compliance risks.
    iv. Ensures adherence to FinCEN AML, PCI DSS, and other relevant regulations.
    v. Leads compliance training and awareness initiatives.
    vi. Manages regulatory examinations and inquiries.
    vii. Establishes and monitors compliance reporting mechanisms.
    viii. Oversees third-party vendor compliance management.
    ix. Acts as the primary point of contact for regulatory bodies on compliance matters.
    x. Provides regular reports to the Board Compliance Committee and senior management.

b. Head of Anti-Money Laundering (AML) Compliance: reports to the chief compliance officer. Key responsibilities include:

    i. Manages the daily operations of the AML program.
    ii. Oversees transaction monitoring, suspicious activity reporting (SAR) processes.
    iii. Ensures customer due diligence (CDD) and enhanced due diligence (EDD) procedures are followed.
    iv. Conducts risk assessments specific to money laundering and terrorist financing.
    v. Stays updated on FinCEN guidelines and regulatory changes.

c. Head of PCI DSS & Data Security Compliance: reports to the chief compliance officer. Key responsibilities include:

    i. Manages the daily operations of the PCI DSS compliance program.
    ii. Ensures implementation and maintenance of security controls.
    iii. Oversees vulnerability management and penetration testing.
    iv. Coordinates incident response related to data breaches.
    v. Ensures compliance with data privacy regulations (e.g., GDPR, CCPA if applicable).

d. Compliance Liaisons (with Business Units): reports to respective business unit head and the CCO. Key responsibilities include:

    i. Act as the first point of contact for compliance queries within their business unit.
    ii. Facilitate the implementation of compliance policies and procedures within their unit.
    iii. Report compliance issues and risks from their unit to the central Compliance Department.
    iv. Promote a culture of compliance within their team.

## GOVERNANCE FRAMEWORK DOCUMENT

The framework's goals are to offer comprehensive business oversight of TechFlow and to ensure that the compliance program is followed in order to sufficiently safeguard the interests of all parties involved. The governance structure and decision-making procedures that apply to TechFlow are described in this framework.

A Chief Compliance Committee (CCO) and other relevant Board committees must be established, along with the Board of Directors. The Board of Directors retains ultimate responsibility for the efficacy of the Compliance Program, and the CCO reports directly to the Board of Directors and Compliance Committee on compliance performance, risks, incidents, and remediation efforts on a quarterly basis at the very least. The budget for the compliance department will be approved by the board of directors, who will also make sure that sufficient staff, technology, and tools are allotted. The organization's board of directors must support a robust compliance and ethics culture.

Existence of Compliance Committee composed of independent directors with relevant expertise in risk management, finance, and legal/regulatory matters. The CCO must attend all committee meetings with the mandate to oversee the design, implementation and effectiveness of compliance program; review and approve key compliance policies and procedures; monitor significant compliance risks and remediation efforts; review findings from internal and external compliance audits; ensure the CCO has sufficient authority, independence, and resources; review and approve the annual compliance plan and budget; receive reports on compliance incidents, investigations, and disciplinary actions. The committee must meet at least quarterly or more frequently as needed if crisis arise, minutes of the meeting must be formally documented.

## REPORTING RELATIONSHIPS AND ACCOUNTABILITY MECHANISMS

a. Reporting Relationships:
    - The CCO will report directly to the board of compliance committee for independence and oversight.
    - The CCO will report administratively to the CEO for operational alignment
    - Compliance department staff will report to the CCO
    - Business Unit Compliance Liaisons will report functionally to the CCO via the relevant Head of Compliance (AML or PCI) and administratively to their business unit heads
    - Whistleblower / Anonymous Reporting: a secure and anonymous channel (e.g., a third-party hotline) will be made available for employees and third-party to report concerns without fear of retaliation. All reports will be triaged and investigated by the compliance department or internal audit for CCO related matters.
b. Accountability Mechanisms:

    - Performance Reviews: Compliance performance will be integrated into the performance reviews of all employees, particularly management and those with compliance responsibilities.
    - Disciplinary Actions: A clear, consistently applied disciplinary policy will be

established for compliance violations, ranging from retraining to termination, irrespective of seniority. This ensures adherence to the "incentives and discipline" element of the US Sentencing Guidelines.

- Responsibility Matrix: A detailed matrix outlining specific compliance responsibilities for key roles and departments will be developed and communicated.
- **Management Certifications:** Key senior managers may be required to periodically certify their department's compliance with relevant policies and procedures.
- Board and Senior Management Responsibility: The Board and senior management will be held accountable for fostering a culture of compliance and ensuring adequate resources for the program.

**TASK 2 – POLICY AND PROCEDURE DEVELOPMENT**

The objective is to establish a comprehensive, structured, and dynamic policy framework that ensures TechFlow Industries' compliance with all relevant regulatory requirements (FinCEN AML, PCI DSS, data privacy) and supports its operational needs.

POLICY HIERARCHY AND CLASSIFICATION SYSTEM

Hierarchy:

- Tier 1 Corporate Compliance Policy: The highest-level document, such as the "Compliance Program Charter" developed in Task 1. It sets the overarching commitment, scope, and principles of compliance for the entire organization.
- Tier 2 Enterprise-Wide Policies**:** Broad policies applicable across all departments and business units, outlining general principles and responsibilities for specific risk areas (e.g., Anti-Money Laundering Policy, Data Security Policy, Code of Conduct).
- Tier 3 Departmental/Functional Policies: More detailed policies specific to a particular department or function, guiding their unique operations (e.g., Customer Due Diligence Policy for Onboarding, Transaction Monitoring Policy for Operations, Incident Response Policy for IT Security).
- Tier 4 Procedures and Guidelines: Highly granular, step-by-step instructions detailing *how* specific tasks are to be performed to comply with policies (e.g., AML Transaction Alert Handling Procedure, PCI DSS System Hardening Procedure).

Classification System:

Policies will be categorized by their primary regulatory or risk area, allowing for easy navigation and management.

- Compliance Category**:**
  - AML/CTF: Anti-Money Laundering, Sanctions, Suspicious Activity Reporting, Customer Due Diligence.
  - PCI DSS/Data Security: Payment Card Industry Data Security Standard, Data Breach Response, Encryption, Access Control.
  - Data Privacy: GDPR (if applicable), CCPA (if applicable), Data Retention, Privacy

Notices.
    - Ethics & Conduct: Code of Conduct, Anti-Bribery & Corruption, Whistleblower Policy.
    - Regulatory Reporting: Specific reporting requirements beyond AML.
    - Third-Party Risk Management**:** Vendor Due Diligence, Oversight.
    - HR Compliance: Employee conduct, data handling for HR.
- Scope: Global, US, Canada, Mexico, Specific Business Unit (e.g., Acquiring, Issuing).

**SAMPLE POLICIES FOR AML AND PCI DSS COMPLIANCE**

Anti-Money Laundering (AML) Policy:

The purpose of this policy is to establish a framework for preventing and detecting money laundering and terrorist financing activities, to ensure compliance with relevant AML laws and regulations, to protect the integrity of the financial system.

Scope: this policy applies to all employees, officers and board of directors of TechFlow, it covers all transactions and activities that may be related to money laundering or terrorist financing.

Policy Statements:

- Enhanced Due Diligence: implementation of enhanced due diligence procedures for higher-risk customers, including potentially exposed persons (PEP), customers from high-risk jurisdictions, and customers engaged in high-risk activities.
- Suspicious Activity Reporting: TechFlow must file SARs whenever they detect transactions or activities that may indicate money laundering, terrorist financing, or other financial crimes. SAR filing is a critical component of the AML framework that provides law enforcement with essential information for investigating financial crimes.
- Ongoing Employee Training: TechFlow must provide ongoing AML training to all employees whose duties requore knowledge of AML requirements. Trainings must be comprehensive, role-specific, and regularly updated to reflect changes in regulations and emerging risks.
- Independent Testing and Auditing: TechFlow must conduct independent testing for their AML programs to assess effectiveness and identify areas for improvement. Testing must be conducted by qualified personnel who are independent of the AML compliance function.
- Currency Transaction Reporting (CTR): TechFlow should file CTRs for cash transactions exceeding $10,000 in a single business day. CTRs help law enforcement track large cash movements that may be associated with criminal activity.
- Record Keeping Requirements: TechFlow must maintain comprehensive records of customer information, transactions, and AML compliance activities. These records are essential for regulatory examinations and law enforcement investigations.

Payment Card Industry Data Security Standard (PCI DSS) Policy:

The purpose of this policy is to protect cardholder data and ensure the security of payment card transactions; to comply with the PCI DSS requirements and maintain a secure environment for

cardholder data; to prevent data breaches and fraud related to payment card information.

Scope: this policy applies to all systems, networks, and applications that store, process, or transmit cardholder data. It covers all employees, contractors, and third-party service providers who have access to cardholder data.

Policy Statements:

- Cardholder Data Storage: TechFlow must implement secure storage practices for cardholder data, including encryption and access controls.
- Cardholder Data Transmission: they must securely transmit cardholder data using encryption and secure protocols.
- Access controls: TechFlow must implement strong access controls to limit access to cardholder data based on the principle of least privilege.
- Regular Security Assessments: TechFlow must conduct regular vulnerability scans, penetration tests, and security audits to identify and address vulnerabilities.
- Incident Response Plan: TechFlow must develop and maintain an incident response plan to address security breaches and data leaks.
- Employee Training: employees must be regularly provided with training on PCI DSS requirements and best practices.
- Vendor Management: TechFlow must ensure that vendors who handle cardholder data comply with PCI DSS requirements.

**POLICY FRAMEWORK DOCUMENT**

The purpose of this Framework is to establish a unified set of organizational policies to ensure compliance with applicable laws and regulations, safeguard sensitive financial data, maintain operational integrity, and support sustainable growth across the United States, Canada, and Mexico.

Scope: this framework applies to all employees, contractors, and third-party partners; all business units and subsidiaries in all countries of operation; all activities involving payment processing, financial data handling, and client interactions

Policy areas:

- Corporate Governance Policy: there must be a board oversight in establishing a Governance, Risk, and Compliance (GRC) Committee to oversee strategic, regulatory, and ethical standards. Code of conduct must be defined for ethical standards, anti-bribery, and anti-money laundering. Disclosure and mitigation processes must be required for all employees and executives for conflict of interest.
- Regulatory Compliance Policy: applicable laws and standards must be set to ensure compliance with PCI-DSS, GDPR, AML, and other payment/financial institution laws in all jurisdictions. A Chief Compliance Officer (CCO) must be appointed with authority to enforce adherence. Conduct semi-annual compliance audits.
- Data Privacy & Protection Policy: data must be categorised as either public, internal, confidential, or highly sensitive. There must be data handling procedures and data retention & disposal in place.

- Cybersecurity Policy: security controls must be put in place such as multi-factor authentication, endpoint security, vulnerability scanning/management. A 24/7 incident response plan with breach notification protocols within regulatory timelines should be defined. Security assessments should be carried out for vendors and partners before onboarding them.
- Operational Risk Management Policy: business continuity & disaster recovery plan must be in place in case of system outages, cyber incidents, and natural disasters. Implement AI-driven fraud detection and suspicious activity reporting. All system changes must be documented, tested, and approved before deployment.
- Human Resources Policy: mandatory compliance and cybersecurity training for all staff regularly, it could be quarterly or annually.
- Anti-Money Laundering & Fraud Prevention Policy: customer due diligence must be carried out, KYC verification at onboarding and periodic re-verification. Proper reporting must be done in any stance of money laundering such as to the SAR.

Roles and Responsibilities:

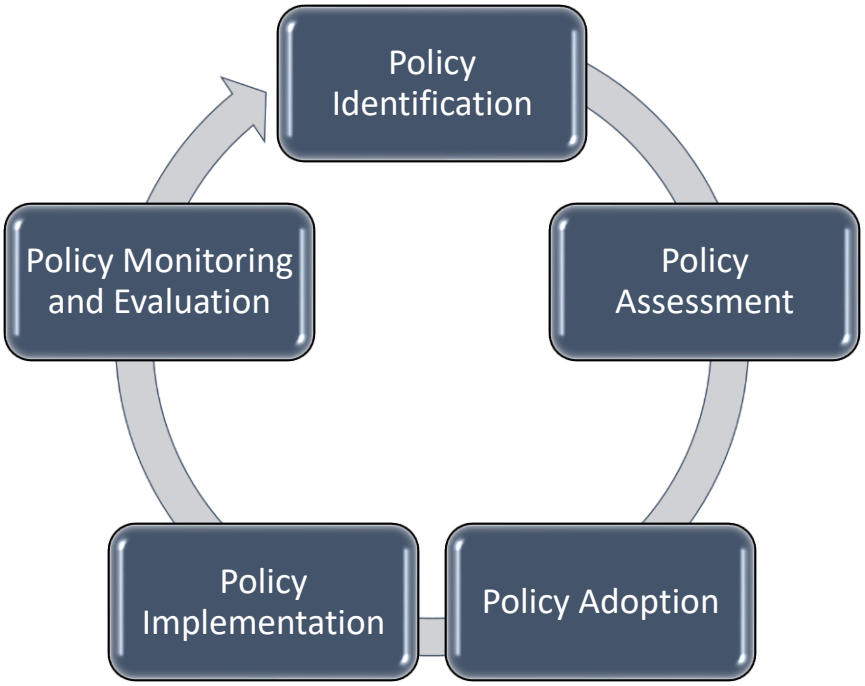
- Board of Directors: approve and oversee policy framework
- Chief Executive Officer (CEO): ensures strategic alignment and adequate resources
- Chief Compliance Officer (CCO): lead compliance efforts, monitor regulatory changes and conduct audits.
- Chief Information Security Officer (CISO): oversee cybersecurity strategy and incident response.
- Business Units Head: enforce policies within their respective units
- Employees: adherence to all policies and reporting of violations.

Enforcement of Policy: if there's a case of violations, it may result in disciplinary action up to and including termination. Severe breaches may lead to regulatory reporting, fines, and legal action.

Review & Update Process: policies must be reviewed by GRC committee and updated for regulatory, technological or operational changes; it must be an annual review. A documented history of changes must be maintained with effective dates.

Supporting Documents:

- Incident response plan
- Business continuity plan
- Data classification plan
- Employee code of conduct
- Vendor risk assessment template




POLICY DEVELOPMENT PROCESS FLOWCHART

POLICY REVIEW SCHEDULE AND RESPONSIBILITIES:

| Policy Category | Policy Title | Policy Owner | Review Frequency |
|---|---|---|---|
| **Tier 1 - Corporate** | Compliance Program Charter | Chief Compliance Officer | Annually |
| **Tier 2 - AML/CTF** | Anti-Money Laundering Policy | Head of AML Compliance | Annually |
| | Sanctions Compliance Policy | Head of AML Compliance | Annually |
| **Tier 2 - PCI DSS** | PCI DSS Compliance Policy | Head of PCI DSS | Annually |
| | Data Breach Incident Response Policy | Head of PCI DSS | Annually |
| **Tier 2 - Data Privacy** | Data Privacy Policy | Head of Data Privacy | Biennially |
| **Tier 2 - Ethics** | Code of Conduct | HR / CCO | Biennially |
| **Tier 3 - Departmental** | Customer Due Diligence Procedure | Head of AML Compliance | Annually |

## TASK 3 – RISK ASSESSMENT AND MONITORING PLAN

The goal is to shift TechFlow from a reactive to a proactive compliance posture by proactively identifying, evaluating, mitigating, and monitoring compliance risks across all of its operations. This plan will offer an organized approach to comprehending TechFlow's risk profile and guaranteeing ongoing compliance with legal requirements, particularly PCI DSS and FinCEN AML.

## COMPLIANCE RISK ASSESSMENT FRAMEWORK

A systematic framework is needed to consistently identify and evaluate risks. Principles like a risk-based approach, which prioritizes resources and efforts based on risk level; comprehensive coverage, which ensures that all relevant compliance areas, including AML, PCI DSS, data privacy, and sanctions, will be accessed; quantifiable and qualitative, which means that risks will be assessed using both quantitative and qualitative measures to provide a holistic view; and accountability, which clearly assigns ownership for risk identification, assessment, and mitigation.

The risk assessment framework must include phases such as the scope definition where specific business units products, services will be identified and assessed; risk identification where risk sources will be reviewed, risks being identified an categorized; control identification assessment where internal controls document (policies, procedures, technology, people) will be designed to mitigate identified risks; risk measurement / rating, risks will be assessed based on their likelihood and impact, both will be combined to determine the inherent risk rating with controls to be considered; mitigation planning will be developed with targeted action plans for high and medium residual risks that are outside TechFlow’s defined risk appetite; reporting and approval, risk assessment findings will be presented with proposed mitigation plans to the relevant stakeholders (CCO, CEO, Compliance Committee); monitoring and review, this must be conducted continuously to monitor the effectiveness of controls and the status of mitigation efforts.

## KEY COMPLIANCE RISKS FOR TECHFLOW

- Anti-Money Laundering (AML) & Counter-Terrorist Financing (CTF) Risks
- Payment Card Industry Data Security Standard (PCI DSS) Risks
- Data Privacy Risks
- Regulatory Reporting Risks
- Third-Party Vendor Compliance Risks
- **Governance & Program Management Risks**

## RISK RATING CRITERIA

Likelihood: being categorised as Very Low (0-10% chance in a year); Low (11-30%); Medium (31-60%); High (61-90%); Very High (91-100% / almost certain)

Impact: such as financial, reputational, operational, technical, regulatory/legal impact. It could be Insignificant with minor disruption, <$100k with minimal reputational damage; Minor with moderate disruption $100k - $500k with local media attention; Moderate with significant

disruption $500k - $2.5M, with regional media and minor regulatory fine; Severe with major disruption $2.5M - $10M with national media and significant regulatory fine & consent order; Catastrophic >$10M leading to business failure, loss of license, criminal charges, global reputational damage.

Risk Rating Matrix (Likelihood vs Impact):

- High Likelihood x Severe/Catastrophic = Critical, which requires immediate action
- Medium Likelihood x Severe Impact or High Likelihood x Moderate Impact = High, requires urgent action.
- Low Likelihood x Severe Impact; Medium Likelihood x Moderate Impact = Medium, requires planned action and regular monitoring.
- Very Low Likelihood x Minor Impact = Low, requires routine monitoring.

**ONGOING MONITORING AND TESTING PROCEDURES**

Beyond the initial risk assessment, continuous monitoring and periodic testing are crucial for ensuring controls remain effective.

a. Ongoing Monitoring Procedures: TechFlow can use real-time sanctions, PEP screening tools, and automated transaction monitoring systems with rule-based and behavioral analytics to identify suspicious patterns. TechFlow can also use ID/IPS and SIEM systems to gather and examine security logs from all important systems. To stop sensitive information, including cardholder data, from escaping the company through unapproved means, TechFlow can also put Data Loss Prevention (DLP) solutions into place. Review high-risk customer accounts on a regular basis, evaluate the quality and efficacy of SAR filings every three months, and keep an eye on regulatory changes and FinCEN advisories to prevent money laundering and terrorist financing. An authorized scanning vendor (ASV) should perform external and internal vulnerability scans every three months, review user privileges and access controls every month or every three months, and examine critical security logs every day in accordance with PCI DSS. TechFlow must regularly hold performance meetings, evaluate the compliance status of key vendors once a year, and keep an eye on their security posture. TechFlow should create and monitor KPIs (Key Performance Indicators) like the efficiency of SAR filings and KRIs (Key Risk Indicators) like unpatched systems and suspicious transaction alerts.
b. Testing Procedures: TechFlow must annually conduct both internal and external audit independently such as the AML audit, PCI DSS audit, data privacy audit. It must be assessed by a Qualified Security Assessor (QSA) to maintain compliance.

**ESCALATION PROCEDURE**

By ensuring that identified compliance issues are promptly addressed at the proper level of authority, clear escalation paths help to keep minor issues from turning into major crises. Timeliness—that is, issues must be escalated without excessive delay—clarity—that is, there must be precise guidelines for when, how, and to whom the issue should be escalated—

documentation—all escalations, actions, and resolutions must be meticulously documented—and accountability—those in charge of each stage of escalation should be assigned.

## TASK 4 – DOCUMENTATION AND REPORTING SYSTEM

## DOCUMENT MANAGEMENT DESIGN

A modern document management system (DMS), ideally integrated within a Governance, Risk, and Compliance (GRC) platform, is crucial for TechFlow. In order to maintain confidentiality and integrity, the document management design must include essential features like a centralized repository for all compliance-related documents, version control that tracks document versions automatically and allows access to historical versions, access controls and permissions that ensure only authorized personnel can view, edit, or approve specific documents, and powerful search and retrieval capabilities with metadata tagging to quickly locate relevant documents for internal use or regulatory requests. It must also include detailed logs of all document actions, which provide an immutable record for audit purposes, automated workflows for document creation, review, approval, and publication processes, and cybersecurity measures that protect sensitive compliance data.

To make management and retention easier, the documents will be categorized according to their lifecycle, content, and level of sensitivity. Policies and procedures, risk assessments, audit and review reports, training materials and records, regulatory communications (notices, filings, and responses), incident and case management records (SARs, security incidents), third-party due diligence & contracts, and board and committee minutes are the categories into which it will be categorized. Sensitivity classifications include restricted, private (such as customer data or SARs), internal use only, and public. It will be categorized under the following regulatory domains: AML, PCI DSS, Data Privacy, and General Corporate Compliance.

A formal document retention policy and schedule will govern how long different types of documents are kept, ensuring compliance with legal and regulatory requirements (e.g., BSA's 5-year retention for AML records) while also managing storage costs and data privacy risks.

### c. Document Retention System:

A formal document retention policy and schedule will govern how long different types of documents are kept, ensuring compliance with legal and regulatory requirements (e.g., BSA's 5-year retention for AML records) while also managing storage costs and data privacy risks.

## COMPLIANCE REPORTING TEMPLATE

Different audiences require different levels of detail and focus. This reporting templates will ensure consistency and efficiency.

Template 1: Compliance Committee report: Reports from the Compliance Committee should be produced on a quarterly or biannual basis and should offer a high-level summary for strategic oversight and decision-making. Important sections of this report should be included, such as the Executive Summary, which must give a thorough overview of the overall compliance posture, important risks, and noteworthy successes and difficulties during that

time; An update on the regulatory landscape that includes a summary of recent or planned changes that affect TechFlow (FinCEN, PCI DSS, Data Privacy); Significant Issues & Incidents; Audit & Review Findings; Policy & Training Updates; Third-Party Compliance; Recommendations & Actions; Program Status Overview with overall compliance score/rating; key risk indicators (KRIs) & trend, identifying top compliance risks and trends.

Template 2: Executive Management Compliance Report: Senior management can oversee daily compliance activities and allocate resources by using the operational and tactical insights provided by the monthly Executive Management Compliance Report. This report should contain key sections like the Executive Summary, which summarizes the month's compliance performance, significant issues, and upcoming priorities. an image of the compliance dashboard showing the key KPIs and KRIs; Performance of the AML Program, including the number of SARs filed and the results of quality reviews; Access control reviews, patching compliance rates, security incident metrics, and internal and external vulnerability scans are all shown by PCI DSS Security Compliance; Policy Adherence Status; Training and Awareness Monthly Completion Rates; Open Issues & Remediation; Regulatory Communications.

Template 3: Business Unit Compliance Report: The monthly Business Unit Compliance Report should provide department heads and line managers with useful information about compliance performance in their respective domains. Key sections like Compliance Performance of Specific Units, which focuses on pertinent KPIs and KRIs for the business unit; Policy Adherence; Team Training Status; Compliance Incidents, which details incidents that originated or affected the unit and their remediation steps; Status of Findings and Unit-Specific Remediation Plans; and Recommendations on what to do should be included.

**KPI FRAMEWORK AND DASHBOARD MOCKUP**

a. Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs):

| Category | KPI (Performance) | KRI (Risk) | Target Example |
|---|---|---|---|
| **AML/CTF** | SAR Filing Timeliness (Avg. days to file after detection) | % of High-Risk Customers without EDD Refresh | < 5 days |
| | % of AML Alerts Resolved within SLA | Volume of Backlogged AML Alerts > 30 days | > 90% |
| | Customer Due Diligence (CDD) Completion Rate for New Accounts | % of Onboarding Applications Flagged for Incomplete CDD | > 98% |
| | Automated Sanctions Screening Hit Rate (True Positives vs. False Positives) | % of Transactions Processed for Entities on Sanctions Lists (if any post-mortem) | High Accuracy |

| | | | |
|---|---|---|---|
| **PCI DSS/Security** | Patching Compliance Rate (% of critical systems patched within SLA) | Number of Critical/High Vulnerabilities Identified in Scans | > 95% |
| | Mean Time To Respond (MTTR) to Security Incidents | Number of Unauthorized Access Attempts to CDE | < 4 hours |
| | % of Employees Completing Annual PCI DSS Security Training | Number of Security Incidents Originating from Human Error | > 95% |
| **Policy/Training** | % of Employees Completing Mandatory Compliance Training | % of Overdue Policy Reviews | > 95% |
| | % of Policies Acknowledged by Relevant Employees | Number of Unaddressed Policy Deviations | > 95% |
| **Issue Management** | % of Compliance Issues Resolved within Stated Timeline | Number of Open Critical/High Compliance Issues | > 90% |
| | Average Days to Close a Compliance Issue | Recurring Compliance Incident Types | < 10 days |
| **Third-Party Risk** | % of Critical Vendors with Completed Compliance Due Diligence | % of Critical Vendors with High-Risk Audit Findings | > 95% |
| | % of Critical Vendors with Valid PCI AoC / Security Attestations | Number of Vendor-Related Security Incidents | > 95% |
| **Audit/Monitoring** | % of Audit Findings Remediated by Due Date | Number of Unresolved Significant Audit Findings | > 90% |
| | Monitoring Control Effectiveness Rating (e.g., % of controls operating effectively) | Number of Material Control Failures Detected | High |

b**.** The Compliance Dashboard Design (Mockup) is a dynamic and interactive visualization tool that can be incorporated into a GRC platform that offers data in real-time or almost real-time. The dashboard's primary sections and widgets include: Overall Compliance Health Score/Status; Compliance Risk Profile, which uses a heatmap to display inherent versus residual risks for the top compliance categories (PCI DSS, AML); Open Issues & Remediation Status, which displays the total number of open issues broken down by severity and status, along with a visual representation of issues by owner or department; Regulatory Changes & Alerts; Audit & Assurance; Third-Party Compliance Overview; Key Performance Indicators (KPIs) Snapshots displaying AML, PCI DSS, and Training KPIs; Users can drill down into underlying data and reports by clicking on a metric or graph.

**REPORTING SCHEDULES AND RESPONSIBILITIES**

**a. Reporting Calendar:**

| Report Type | Audience | Frequency | Primary Owner (Accountable) | Contributors (Responsible) |
|---|---|---|---|---|
| **AML SAR Filings** | FinCEN | As required | Head of AML Compliance | AML Analysts |
| **PCI DSS Attestation/ROC** | PCI SSC, Banking Partners | Annually | Head of PCI DSS Compliance | IT Security, IT Operations, External QSA |
| **Executive Management Compliance Report** | CEO, Executive Leadership | Monthly | Chief Compliance Officer | Heads of AML, PCI DSS, Regulatory Compliance |
| **Board Compliance Committee Report** | Board Compliance Committee (Board of Directors) | Quarterly | Chief Compliance Officer | Heads of AML, PCI DSS, Regulatory Compliance, Internal Audit |
| **Business Unit Compliance Report** | Business Unit Heads, Department Managers | Monthly | Business Unit Compliance Liaison | Business Unit Staff, Compliance Department Support |
| **Compliance Risk Register Review** | CCO, Executive Management, Board Compliance Committee | Annually (full), Quarterly (updates) | Chief Compliance Officer | All Department Heads, Risk Management Team, Compliance Department |
| **Compliance Training Completion Report** | HR, Managers, CCO | Monthly | HR / Compliance Training Lead | All Managers (for their teams) |
| **Third-Party Compliance Review Report** | CCO, Procurement, Relevant Business Unit | Quarterly | Head of Regulatory Compliance | Third-Party Risk Analyst, Business Unit Managers |
| **Internal Audit Report (Compliance Focus)** | Audit Committee of the Board, CCO | Annually | Head of Internal Audit | All Departments (audited areas) |
| **Regulatory Change** | CCO, Legal, Relevant Business | As needed | Head of Regulatory | Legal Department, |

| | | | | |
|---|---|---|---|---|
| **Impact Assessment** | Units | | Compliance | Business Unit Leads |

**TASK 5 – IMPLEMENTATION ROADMAP**

The implementation of TechFlow Industries' compliance program will follow a phased approach, prioritizing immediate regulatory demands while systematically building a robust and sustainable framework for the long term.

90-DAY EMERGENCY RESPONSE PLAN: the first 90 days are crucial for demonstrating significant progress to regulators (FinCEN and PCI SSC) and mitigating the most critical identified risks, this phase focuses on quick wins and foundational elements.

| Activity | Key Deliverable | Dependencies | Responsible Teams | Estimated Duration (Days) |
|---|---|---|---|---|
| Week 1-2: Appoint CCO & Establish Core Compliance Team | Formal CCO Appointment & Initial Team Structure | Board Approval, HR Support | Board, CEO, HR | 14 |
| Week 1-3: Rapid Risk Assessment & Gap Analysis (Focus: AML & PCI) | Updated Risk Register & Gap Report | New CCO, Initial Compliance Team | CCO, Risk, IT Security | 21 |
| Week 2-5: Review & Update Critical AML & PCI Policies | Revised AML & PCI DSS Policies/Procedures V1.0 | Rapid Risk Assessment Findings | Compliance, Legal, IT Security | 28 |
| Week 3-6: Setup Centralized Document Repository | Basic Document Management System Operational | IT Infrastructure, Initial Compliance Team | IT, Compliance | 28 |
| Week 4-8: Initial Mandatory Employee Training Rollout | Acknowledged & Completed Core Training | Updated Critical Policies, HR L&D | HR, Compliance | 35 |
| Week 5-9: Enhance AML Transaction Monitoring Rules & Processes | Optimized Rules & Alert Review Workflow | Current System Capabilities, AML Team | AML Compliance, IT | 35 |

| | | | | |
|---|---|---|---|---|
| Week 6-10: PCI DSS Vulnerability Management Sprint | Remediation of Top Critical/High Vulnerabilities | IT Security Team Availability, Tools | IT Security | 35 |
| Week 9-12: Prepare Regulatory Remediation Plan & Report | Comprehensive Progress Report for FinCEN & PCI SSC | All preceding activities, Data from monitoring | CCO, Legal, Executive Mgmt | 21 |

90-Day Plan Success Metrics: CCO appointment; identification of core AML & PCI compliance leads; 100% of the PCI DSS and identified core AML policies have been examined, revised, and approved by the board; The centralized repository contained 80% of the important compliance documents, such as new policies and important incident logs; 50% of the current backlog of AML alerts has been reduced, and the first steps to improve the transaction monitoring rules have been taken. 75% of PCI DSS vulnerabilities that are critical and high severity have been fixed; 80% of relevant employees have completed the required core compliance training (PCI DSS fundamentals, AML awareness); formal delivery of the progress report and comprehensive remediation plan to FinCEN and PCI SSC by the 90-day deadline.

12-MONTH IMPLEMENTATION ROADMAP: this roadmap extends beyond the emergency response, focuses on building a comprehensive, sustainable, and continuously improving compliance program. This implementation is a phased approach and distributed into three phases.

Phase 1 (1-3 Months): this phase represents the emergency response and stabilization phase focusing on immediate risk mitigation, foundational governance, critical policy updates, initial training and regulatory reporting.

Phase 2 (4-9 Months): this phase represents the program build-out and integration focusing on expanding the compliance framework, integrating technology, developing advanced reporting and deeper role-specific training. Key activities of this phase include; completion of policy framework; GRC platform selection & implementation; automated data integration; advanced transaction monitoring; comprehensive training program; third-party risk management program; internal audit & control testing.

Phase 3 (10-12 Months): this phase represents the optimization and continuous improvement phase focusing on refining processes, enhancing reporting and analytics, embedding compliance culture, and preparing for future challenges. Key activities of this phase include; annual compliance program effectiveness review; advanced analytics & reporting; scenario planning & crisis simulation; compliance culture reinforcement; technology optimization; prepare for next regulatory cycle.

**Critical Path Activities and Dependencies (12-Month View):**

| Activity | Key Deliverable | Dependencies | Responsible Teams |
|---|---|---|---|
| Overall Governance & Leadership | Operational Compliance Committee, CCO fully staffed | Board Appointment of CCO, Budget Approval | Board, CEO, HR |
| Comprehensive Risk Assessment | Enterprise-wide Compliance Risk Register | CCO, Dedicated Risk Function, Business Unit Input | CCO, Risk, Business Units |
| Complete Policy & Procedure Framework | Approved, Published Policies & Procedures | Risk Assessment, Regulatory Requirements | Compliance, Legal, Business Units |
| GRC Platform Full Implementation | Integrated Compliance Management System | IT Infrastructure, Vendor Selection, Data Integration | IT, Compliance |
| Automated Data Feeds & Reporting | Real-time Compliance Dashboards & Alerts | GRC Platform, Core Business Systems | IT, Compliance, BI |
| Full Employee Training Program | Role-specific Training Modules & Completion | HR L&D Platform, Policy Framework | HR, Compliance |
| Robust Monitoring & Testing | Regular Control Testing, Audit Reports | Policy Implementation, IT Tools, Internal Audit | Compliance, Internal Audit |
| Third-Party Risk Management Program | Operational Vendor Due Diligence & Monitoring | Policy Development, Procurement, IT Security | Compliance, Procurement |
| Regulatory Engagement & Liaison | Proactive Communication & Timely Filings | Data & Reporting Capabilities, Legal Counsel | CCO, Legal, Executive Mgmt |
| Continuous Program Improvement | Annual Effectiveness Review, Enhanced Capabilities | Audit Findings, KRI Trends, Regulator Feedback | CCO, Executive Leadership |

RESOURCE AND BUDGET REQUIREMENT

Personnel such as the CCO, the Head of AML Compliance, the Head of PCI DSS & Data Security Compliance, compliance analysts, IT security analysts, GRC specialists, internal audit, and legal counsel are among the resources needed. Technologies like SIEM, Data Loss

Prevention Solution, Automated Sanctions Screening Tools, Enhanced AML Transaction Monitoring System, GRC Platform, Secure Document Management System, and Learning Management System (LMS). The following outside services are needed: staff augmentation, independent AML auditing, qualified security assessment (QSA), compliance consulting firm, and legal advisory.

**Budget Estimates (Illustrative Annualized Costs):**

| Category | Estimated Cost (Annualized, in USD) | Notes |
|---|---|---|
| Personnel (New Hires) | $1,000,000 - $2,500,000 | 5-8 FTEs (CCO, AML/PCI Heads, Analysts, Specialists). Varies greatly depending on market rates, seniority, and experience (for example, a highly experienced CCO will be more expensive). includes pay and benefits. |
| GRC Platform (Licenses) | $150,000 - $400,000 | Annual subscription for a robust, enterprise-grade GRC platform. |
| GRC Platform (Implementation) | $200,000 - $700,000 (One-time) | Professional services for configuration, integration with existing systems, data migration, user training. This is a significant upfront cost. |
| AML/Sanctions Systems | $100,000 - $500,000 | Licenses, upgrades, and maintenance for advanced transaction monitoring and sanctions screening solutions. |
| Security Tools (SIEM, DLP, Scanners) | $75,000 - $250,000 | Annual licenses and maintenance for comprehensive security monitoring, vulnerability management, and data loss prevention tools. |
| External Audits/Assessments | $100,000 - $300,000 | Annual PCI DSS QSA assessment, independent AML audit, and potentially other specialized compliance audits. |
| Consulting/Legal Services | $100,000 - $400,000 | Initial remediation consulting, ongoing specialized legal advice, ad-hoc expert support for specific compliance challenges. This will be higher in the first year and can be reduced. |
| Training & Awareness | $30,000 - $100,000 | Development of custom training content, LMS licensing, external trainers, and ongoing awareness campaigns. |
| Contingency (15-20%) | $200,000 - $800,000 | For unforeseen costs, emergent regulatory requirements, scope changes, or additional staffing needs. Crucial for a transformation project. |
| TOTAL | **$1,755,000 -** | This is a substantial investment, reflecting the severity of the |

| | | |
|---|---|---|
| ESTIMATED ANNUAL (Excl. GRC Impl.) | **$4,850,000+** | identified deficiencies and the scale of the required transformation. The first year will be higher due to one-time implementation costs. This represents a significant portion of the $2.5M in prior legal/consulting fees and potential fines. |

CHANGE MANAGEMENT STRATEGY

Successfully integrating the new compliance program into TechFlow's operations and culture requires effective change management. Among the tactics should be: Strong Leadership Sponsorship, in which the CEO and board will openly support the compliance transformation; Stakeholder Engagement: Early on in the compliance process, the stakeholders need to be actively involved; Communication & Transparency: To foster understanding and support, it is imperative to proactively communicate the reasons behind the changes. Training & Capability Building: offer thorough, role-specific instruction that is applicable to everyday duties and practical; Feedback and Loops; Reinforcement & Recognition; and Resistance Management.

**SUCCESS METRICS AND MEASUREMENT PLAN**

Long-term success metrics include: successful removal from probationary status on the PCI SSC and full compliance with PCI DSS; no new significant regulatory findings or penalties pertaining to AML, PCI DSS, or data privacy; favorable results from independent AML program reviews; and timely filing of all regulatory documents. Risk will be decreased, and security incidents and compliance breaches will occur less frequently and with less severity. Automation of compliance procedures has increased, and internal audit results for compliance-related areas have improved. An increase in affirmative answers to employee surveys about ethical culture and compliance awareness.

APPENDIX A: COMMUNICATION PLAN

| Audience | Purpose | Key Messages | Channels | Frequency | Owner |
|---|---|---|---|---|---|
| Board of Directors & Executive Leadership | Secure continued sponsorship, update on progress & risks | Urgency of transformation, strategic importance, progress against roadmap, resource needs, impact on financial health/IPO. | Formal Reports, Executive/Board Meetings, Workshops | Bi-weekly (initial), Monthly/Quarterly | CCO, CEO |
| All Employees | Awareness, build culture, behavioral expectations | "Why" we're doing this (regulatory pressure, protecting jobs/business), new compliance framework, their role, importance of reporting concerns, non-retaliation. | Company-wide Emails, Town Halls, Intranet News, Posters | Monthly (ongoing), Ad-hoc | CCO, HR, Marketing |
| Managers/Team Leads | Enablement, cascade information, enforce policies | Specific changes impacting their teams, new tools/systems, reporting requirements, how to support teams, disciplinary guidelines, issue escalation. | Team Meetings, Manager Briefings, Dedicated Training | Bi-weekly/Monthly | Compliance Liaisons, CCO |

| | | | | | |
|---|---|---|---|---|---|
| IT/Tech Teams | Collaboration, technical requirements | System changes, integration needs, security protocols, data access for compliance, support for GRC platform. | Project Meetings, Technical Workshops, Jira/Confluence | Weekly (initial), Bi-weekly | Head of IT, Compliance |
| Customers | Maintain trust, transparency (general) | Reinforce commitment to data security and privacy, recent enhancements to protect their information (general terms, no crisis details). | Website Updates, Privacy Policy Updates, Client Communications | As needed | Marketing, Legal |
| Regulators (FinCEN, PCI SSC) | Transparency, progress, issue resolution | Detailed remediation plan, consistent updates on progress, proactive disclosure of challenges, data requests. | Formal Submissions, Direct Correspondence, Scheduled Meetings | As required, Quarterly | Legal, CCO |

APPENDIX B: RESPONSIBILITY MATRIX

| Report/Activity | CCO | Head of AML | Head of PCI-DSS | Head of Reg. Compliance | Internal Audit | Business Unit Heads | Legal Dept. | IT Security | HR | Compliance Committee |
|---|---|---|---|---|---|---|---|---|---|---|
| Executive Mgmt Report | A | R | R | R | C | I | C | I | I | I |
| Committee Report | A | I | I | I | C | I | C | I | I | R |
| AML SAR Filings | A | R | - | C | I | I | C | I | - | I |
| PCI DSS Attestation | A | - | R | C | C | I | C | R | - | I |
| Compliance Risk | A | R | R | R | C | C | C | C | C | I |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Register | | | | | | | | | | |
| Policy Updates/Approval | A | R | R | R | C | C | C | C | C | A |
| Training Completion | A | I | I | I | C | R | - | - | R | I |
| Third-Party Review | A | R | R | R | C | C | C | C | - | I |
| Regulatory Inquiries | A | R | R | R | C | C | R | R | - | I |
| Incident Response Report | A | R | R | C | I | R | C | R | I | I |

**Responsibility Matrix (RACI - Responsible, Accountable, Consulted, Informed):**

- **Responsible (R):** The individual(s) who perform the task.
- **Accountable (A):** The one person ultimately answers for the correct and complete execution of the task. (There should only be one A per task/report).
- **Consulted (C):** Individuals or groups whose opinions are sought, typically subject matter experts.
- **Informed (I):** Individuals or groups who are kept up-to-date on progress or decisions.