FintexCorp: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope: The scope of this audit is defined as the full security program and infrastructure used by FintexCorp, a digital financial services provider. This includes their cloud-based platforms, APIs, mobile applications, payment systems, internal network components, and sensitive customer data management practices.

Goals:

- Identify all key assets and systems used by FintexCorp
- Assess technical security controls and configurations
- Evaluate compliance with industry regulations including **PCI DSS** and **SOC 2**
- Recommend mitigations to strengthen FintexCorp's cybersecurity posture, focusing on **transactional integrity, access control, and data protection**

Current assets

Assets managed by the FintexCorp IT and DevOps teams include:

- Cloud-hosted payment processing infrastructure (AWS Lambda + API Gateway + DynamoDB)
- Public-facing APIs for third-party merchant integrations
- Customer mobile app and administrative web portal
- PostgreSQL and NoSQL databases for transaction logs and user data
- Tokenization service for credit card storage
- Application source code hosted in GitHub Enterprise
- CI/CD pipeline deployed with GitHub Actions and Terraform
- AWS KMS for encryption key management
- Firewall rules via AWS Security Groups
- Internal VPN for admin panel access
- Antivirus software on employee endpoints

- Slack + Google Workspace for team communication
- Monitoring via CloudWatch and manual alerts
- No formal SIEM in place
- No current implementation of intrusion detection or network segmentation
- MFA enforced on production cloud accounts, but not across all internal systems
- Password policies weak and not centralized
- Backups are configured but restoration processes are undocumented
- No disaster recovery plan (DRP) tested or formalized
- Logs stored in S3 without automated analysis

Risk assessment

Risk description

FintexCorp is currently operating without some of the essential security controls expected in fintech environments. Although tokenization and encryption mechanisms are partially implemented, gaps in identity management, detection capabilities, and formal response plans introduce considerable risk to customer data and transactional integrity.

Control best practices

To align with PCI DSS and SOC 2, FintexCorp should:

- Enforce **least privilege** and **role-based access** controls for all internal systems
- Require **MFA** across all systems, not only production cloud services
- Formalize and test a **Disaster Recovery Plan** (DRP)
- Implement a **centralized password management system**
- Deploy a **SIEM** for real-time monitoring and incident detection
- Enhance encryption mechanisms and ensure **tokenization is irreversible**
- Harden public APIs with **rate limiting, authentication, and audit logging**
- Classify and inventory all data, especially financial and personally identifiable information (PII)

Risk score

On a scale of 1 to 10, the risk score is **8**, primarily due to missing detection capabilities, weak identity management controls, and incomplete compliance with PCI DSS requirements.

Additional comments

The following weaknesses and gaps were observed during the assessment:

- Public APIs lack integrated DDoS protection and are vulnerable to abuse
- No SIEM or IDS is in place for real-time anomaly detection
- Developers have access to production environments via shared credentials
- PCI DSS controls are only partially enforced — tokenization is used, but sensitive data is accessible internally without full encryption
- The backup process is automated, but no documented **restoration plan** exists
- Password complexity is not enforced across all admin interfaces
- DevOps pipelines lack automated security testing stages
- VPN access is not MFA-protected
- Sensitive logs are stored but not monitored or analyzed
- No formal business continuity strategy has been established