SafeInvest Scope, Goals and Risk Assessment

Introduction

This scenario is based on a fictional company:

Project Background: SafeInvest is a fast-growing fintech startup in the UAE, offering digital wealth management, mobile trading, and cross-border payment services. What started as a platform for local investors has quickly gained traction across the region thanks to its simple and innovative approach.
As the business grows, the CTO recognizes importance of keeping the platform secure and protecting the sensitive financial and personal information that customers entrust to SafeInvest. She understands that this growth means greater responsibility, and proactively taking steps to ensure we have a solid plan for both business continuity and compliance, which is why she has initiated an internal IT audit to get a clear picture of our current security posture.

The goal of the audit is to review the scope of operations, identify key digital assets, and assess the risks they might face, uncovering vulnerabilities that could lead to data breaches, financial losses, or regulatory fines. The audit will also evaluate how SafeInvest is meeting key compliance standards like ISO 27001, PCI DSS, and the UAE Central Bank Regulations, so the company can take clear steps towards its security and strengthening its overall governance.

Audit Scope

The scope of this internal audit covers SafeInvest's overall security program, including its cloud infrastructure, internal systems, digital assets, and policies related to data protection, access control, and incident response. It also includes all processes and procedures tied to the company's compliance with ISO 27001, PCI DSS, and UAE Central Bank Information Security Regulations.

Goal of this Audit:

- Review and document all key digital assets and systems managed by the IT and security teams.
- Assess current controls and policies to determine how well they align with relevant security and compliance standards.
- Complete the controls and compliance checklist to identify any missing or weak controls.
- Highlight gaps or vulnerabilities that could lead to security incidents or non-compliance.
- Provide clear, actionable recommendations to help SafeInvest strengthen its security posture and ensure compliance moving forward.

Assets Identified

Assets managed by the IT Department at SafeInvest:

- **Customer Information Database:** A centralized repository that stores sensitive customer data, containing personally identifiable information (PII), financial data, and investment profiles of SafeInvest clients used across the platform.
- **Mobile and Web Trading App:** the mobile and web application of the trading system, that customers use to manage their investments, view market trends, and place trades.
- **Payment and Remittance System:** handles all financial transactions such as card payments, banking API integrations, and cross-border remittance services.
- **User Access and Authentication System:** manages login workflows, session management, password resets and MFA (multi-factor authentication).
- **Financial Transaction Logs:** keeps track of all financial activities, required for audits, dispute resolution, and regulatory reporting.
- **Dev/Test Environment:** the space where development team build and test new features before releasing them into production. This includes staging servers, code repositories, and CI/CD pipelines.
- **Cloud Infrastructure:** SafeInvest runs most of its backend systems on the cloud, virtual servers, storage services, managed databases, backup solutions, and orchestration tools. This infrastructure supports both frontend and backend operations.
- **Employee Devices:** Workstations, laptops, mobile phones, secure USBs, and other endpoint devices used by internal staff.
- **Public Company Website**: the main marketing site of SafeInvest MENA, used for marketing, onboarding new users, and communicating service updates. It also links customers to support and account management portals.

Risk Assessment

The following table presents the summary of the initial risk assessment findings as reported by SafeInvest's IT team.

Asset	Threat	Vulnerability	Likelihood	Impact	Risk Level
Mobile and Web Trading Application	Unauthorized Transactions	Insufficient multi-factor authentication, session management weaknesses; API exposure vulnerabilities	Medium	High	High
Payment Processing System	Fraudulent Transactions	No tokenization of payment data, inadequate logging; lack of proper isolation between payment and other systems	Medium	High	High
Digital Investment Platform	DDoS Attack	Single points of failure in server architecture; lack of dedicated DDoS mitigation controls	Medium	High	High

Asset	Threat	Vulnerability	Likelihood	Impact	Risk Level
Customer Database	Data Breach	Weak access controls, limited encryption; potential injection flaws in database queries	High	Critical	High
Customer Accounts	Account Takeover	Weak password policies; limited MFA usage; susceptibility to phishing	High	Medium	High
Transaction Logs	Data Tampering	Inadequate logging practices; lack of integrity checks and monitoring tools	Medium	Medium	Medium
Development & Test Environment	Malicious Code Injection	Lack of formal secure coding guidelines; inconsistent code reviews	Low	High	Medium
Cloud Infrastructure & Storage	Unauthorized Access	Misconfigured access controls on cloud resources; weak key management; lack of automated security monitoring	Medium	Medium	Medium
Employee Workstations	Malware Infection	Outdated antivirus/malware solutions, limited security awareness training on phishing.	Medium	Low	Low
Company Website	Defacement	Outdated web application framework; infrequent patching; minimal web application security testing.	Low	Medium	Low

Observations on Current Control Practices

During our review, we observed that while the organization has made progress in implementing security measures, there are still some gaps in how these assets are tracked and classified, particularly enforcing controls. This is critical because understanding what assets exist, their value, and how they contribute to business continuity helps determine the impact should they be compromised.

In addition to these core issues, we noted several specific areas that require improvement:

- **Access Management:** Currently, all employees have broad access to internal data, which increases the risk of unauthorized data exposure. Implementing stronger controls, such as role-based access and multi-factor authentication, is highly recommended.
- **Data Encryption:** While some sensitive financial data is encrypted, the practice is not consistent across all systems. Certain cloud storage areas and transaction logs remain unencrypted, which puts customer payment information at risk.

- **Compliance Gaps:** Although, SafeInvest has some security policies in place, they do not fully align with modern standards. For instance, the current password policies are minimal, and there is no centralized management system in place. This could lead to significant compliance issues and fines down the line.
- **Incident Detection & Recovery:** Basic defenses such as firewalls and antivirus software are in place; however, the absence of an intrusion detection system (IDS) and a structured disaster recovery plan leaves the company vulnerable in the event of an incident.
- **Legacy Systems:** Some older systems are still in use and lack a regular maintenance schedule. These systems rely on human monitoring, making them potential weak links in the overall security chain.
- **Physical Security:** Although physical security measures (locks, CCTV, fire detection) are effective at office locations, the digital environment lacks equivalent protections, which could allow cyber threats to go undetected.