RISK ASSESSMENT – FINAL REPORT

Company: Fin Analytics

Assessor: Pavel Pecheniuk

Date: 21.08.2025

1. Company Profile

Name: Fin Analytics

Location: Berlin, Germany

Industry: FinTech

Number of employees: 70

Business: Provides cloud-based financial analytics and investment portfolio management tools for small and medium businesses.

Regulatory Environment:

- GDPR (General Data Protection Regulation);
- MiFID (Markets in Financial Instruments Directive) II.

---

2. Critical Assets, Threats and Vulnerabilities

2.1 Critical Assets

Table 1 represents **the inventory** of the main critical assets of Fin Analytics.

Asset	Sensitivity Level	Comments	Exploit Notes
Client Financial Data	Confidential	Financial records & PII (personally identifiable information), which fall under protection of GDPR & MiFID	Regulatory fines, fraud, reputational damage
Web + Mobile Applications	Confidential	Primary customer-facing interfaces responsible for portfolio management and analytics	Large breach of client data
Cloud Infrastructure	Confidential	Core backbone hosting workloads and databases	Data breach
Internal Network	Internal	Employee laptops, internal file servers, office Wi-Fi	Could be exploited as entry point

Employees	Internal	Workforce with access to sensitive client data	Privileged access abuse

Table 1. Critical Assets Inventory

2.2 Threats

The following threats are crucial for the critical assets considered in the 2.1:

- **External Cyberattacks (Web App: Man-in-the-Middle, SQL injection; Mobile App: API abuse, Reverse engineering):** perpetrators will target sensitive client data, including personal and financial, for fraud, resale or blackmail.
- **Cloud Misconfiguration:** misconfigured or compromised cloud leads to exposure of databases and storage buckets.
- **Insider Threats:** negligent or malicious employees expose sensitive data via internal network endpoints.
- **Ransomware:** encrypting internal or cloud-stored files for subsequent requirement of the payment of a ransom fee for the deciphering keys.
- **Social Engineering:** misdirection of negligent or unaware employees to steal credentials necessary to advertently enter the system.

2.3 Vulnerabilities

Vulnerabilities that are likely to be exploited by threat actors are listed below:

- **Lax Access Control (Weak Passwords, no MFA (Multi-Factor Authentication)):** usage of simple and reused passwords by employees, admin and privileged accounts are severely unprotected without MFA.
- **Unpatched Systems:** delayed security updates on web server, software and endpoints.
- **Elevated User Privileges:** lack of RBAC (role-based access control), violation of the least privilege principle.
- **Cloud Misconfiguration:** public storage buckets with insufficient access restrictions.

3. Risk Assessment

To define and assess risks, **a risk register** represented in Table 2 was created to consider several risk scenarios and estimate the probability of the risk and the impact this risk will bring. Risks then are prioritized.

Likelihood scale: 1 – Low, 2 – Medium, 3 – High. Impact scale: 1 – Low, 2 – Moderate, 3 – Medium, 4 – High, 5 – Extreme.

Asset	Threat	Vulnerability	Likelihood (1-3)	Impact (1-5)	Risk Level = L*I
Client Financial Data	External Attack	Cloud Misconfiguration	High (3)	Extreme (5)	Critical (15)
Mobile App	API Abuse	Poor Authentication/ Authorization	High (3)	Extreme (5)	Critical (15)
Employee Accounts	Phishing	Weak Password	High (3)	High (4)	High (12)
File Server	Ransomware	Unpatched OS	Medium (2)	High (4)	High (8)
Internal Data	Insider Threat	Unenforced Least Privilege	Medium (2)	High (4)	High (8)
Web App	SQL Injection	Unpatched Software	Medium (2)	Medium (3)	Medium (6)

Table 2. Risk Register

---

4. Risk Prioritization & Ranking

Here **the simplified risk heat map** is presented, where the risks are ranked to focus on the highest ones which require immediate actions.

- **Critical:** Client financial data exposure due to cloud misconfiguration and insecure authentication/authorization.
- **High:** Employees' weak credentials resulting in the vulnerability towards phishing, ransomware on file server, lack of least privilege principle leading to the higher probability of insider threats.

- **Medium:** Web application exploitation risk by external attacks.

---

5. Recommended Mitigation Strategies

1) Client Financial Data

- Implement access control measures, including SoD (Separation of Duties).
- Maintain secure and proper cloud configuration.
- Ensure strong transit + storage data encryption.
- Enable logging and monitoring of all access.

2) Mobile Application

- Enforce stronger login procedure via combination of SSO (Single Sign-On) and MFA.
- Ensure all communication between the app and the server is encrypted and protected against interception.
- Conduct regular abuse-targeted monitoring.

3) Employee Accounts

- Conduct security awareness training with focus on resilience to social engineering attacks.
- Employ MFA for all privileged accounts.
- Harden password policies.

4) File Server

- Ensure that systems are patched and timely updated.
- Conduct regular offline backups.
- Use endpoint protection with ransomware detection.

5) Insider Threat

- Implement RBAC and enforce least privilege.
- Monitor and analyse user activity.

6) Web Application

- Conduct continuous security testing by means of penetration testing.
- Deploy WAF (Web Application Firewall).
- Apply regular security patches.

---

6. Summary

Conducted risk assessment of Fin Analytics identified five primary risks, with client financial data exposure due to cloud infrastructure misconfiguration and insecure authentication/authorization of mobile application being the most critical. Immediate actions must be concentrated on improvement of security and operation of cloud infrastructure and mobile app, implementation of access controls and MFA and ensuring proper patch management. These measures will:

- reduce the likelihood of security incidents, including data breaches.
- enhance GDPR compliance: MFA for privileged accounts reduces risk of credential theft and supports GDPR Article 32 (Security of Processing).

---

7. Next Steps

- Develop continuous monitoring for cloud and internal infrastructures.
- Prioritize critical and high risks for remediation in the next quarter.
- Schedule risk re-assessments and update threat intelligence regularly to combat with the expanding field of threats.