**Compliance Risk Brief – FinSure Capital**

This internal brief highlight key compliance risks identified during the Q1 operational review. Each point below requires internal attention and cross-functional collaboration to mitigate regulatory exposure and ensure legal compliance.

**1. Incomplete KYC Documentation**

* Several customer profiles opened in January–February 2025 are missing proof of address and ID verification.
* This poses a direct AML/KYC violation risk.
* Regulatory bodies (e.g., FCA) may penalize for onboarding non-compliant clients.
* Risk Level: High
* Involved Department: Customer Support / Compliance
* Action Needed: Review all client files from Q1 and enforce verification protocols.

**2. Outdated Data Privacy Policy (GDPR/CCPA)**

* The current privacy policy hasn’t been updated since August 2022.
* Recent regulatory changes (GDPR, CCPA amendments) are not reflected.
* Risk Level: Medium
* Involved Department: Legal / Marketing
* Action Needed: Engage Data Privacy Consultant to review and revise documentation.

**3. Lack of Documentation for Internal Audit Procedures**

* Audit process followed by Finance is not fully documented.
* Missing audit trail for several transactions above $10,000.
* Risk Level: Medium-High
* Involved Department: Finance / Internal Audit
* Action Needed: Standardize internal audit procedures and develop clear documentation for high-value reviews.

**4. Weak Access Controls on SaaS Tools**

* Several ex-employees still have active credentials to internal CRM and analytics platforms.
* Risk Level: High (Cybersecurity & Data Access)
* Involved Department: IT / Security
* Action Needed: Conduct user access audit and implement offboarding checklist.