15. Risk Management Approach

15.1 Our Risk Philosophy

E-invoicing compliance is not just a technology integration — it is a regulated process where delays or failures can directly impact revenue, reputation, and legal standing. Softrust and Bluelight treat risk management as an **active discipline**, built into every phase of delivery and ongoing operations.

<diagram: Risk management cycle — Identify → Assess → Mitigate → Monitor → Review → Improve>

15.2 Risk Identification

We proactively identify risks across three dimensions:

- **Technology Risks** – ERP integration complexity, regulator changes, infrastructure failures.
- **Process Risks** – incorrect data mapping, reconciliation errors, insufficient testing.
- **People Risks** – lack of user adoption, inadequate training, unclear accountability.

15.3 Risk Assessment Framework

- **Likelihood Scale**: Rare, Unlikely, Possible, Likely, Almost Certain.
- **Impact Scale**: Low (minor operational issue), Medium (business disruption), High (financial penalty or compliance breach), Critical (regulatory non-compliance).
- Risks are scored as **Likelihood x Impact**, then plotted on a heat map for visibility.

<diagram: Heat map grid showing risks plotted by likelihood vs impact>

15.4 Top Compliance Project Risks and Mitigations

Risk 1: FIRS Specification Changes During Project

- *Impact*: Could require ERP rework and delay go-live.
- *Mitigation*: SmartAPI absorbs schema changes centrally via versioning and feature flags. No ERP modification required.

Risk 2: Poor Master Data Quality (TINs, HS Codes, Tax Codes)

- *Impact*: Rejected invoices, compliance gaps.
- *Mitigation*: Early master data validation, resource library sync with FIRS, Finance workshops for data cleanup.

Risk 3: ERP Integration Delays

- *Impact*: Slippage in SIT/UAT timelines.
- *Mitigation*: Pre-built templates for SAP PI/PO and CPI iFlows, dedicated integration engineers, fallback via Email Connector.

Risk 4: System Downtime at Go-Live

- *Impact*: Invoice submissions blocked, revenue recognition delayed.
- *Mitigation*: Cutover rehearsals, rollback plan, hypercare with 24x7 monitoring, autoscaling SmartAPI.

Risk 5: Security Incidents (Certificate Expiry, Unauthorized Access)

- *Impact*: Compliance breach, reputational damage.
- *Mitigation*: Certificate expiry alerts at T-30, T-7, T-1; RBAC; MFA; SIEM integration; quarterly access reviews.

Risk 6: User Adoption Resistance

- *Impact*: Manual workarounds, compliance bypass.
- *Mitigation*: Training sessions, knowledge transfer, Finance liaison support, dashboards to reduce manual effort.

15.5 Risk Governance Model

- **Risk Register** maintained from project kickoff, updated weekly by PMO.
- **Steering Committee** reviews top risks and mitigation actions bi-weekly.
- **Early Warning Indicators** monitored (rejection rates, queue backlogs, latency spikes).
- **Playbooks** activated for high-impact risks (e.g., regulator outage, mass rejection event).

15.6 Example Risk Heat Map

Likelihood \ Impact	Low	Medium	High	Critical
Rare	Minor UI bug	–	–	–
Possible	User training gap	Data mapping error	–	–
Likely	ERP delay	FIRS spec change	Downtime risk	–
Almost Certain	–	–	–	Security incident if no certificate monitoring

<diagram: Risk heat map visual showing risks grouped into red, amber, green zones>

15.7 Continuous Risk Monitoring

- Dashboards show live risk indicators: clearance rate drops, abnormal latency, rising rejection codes.
- Daily stand-ups in project phase include risk review.
- In steady state, risks reviewed quarterly with KPI trends.
- Lessons learned feed into continuous improvement backlog.

15.8 Why Our Risk Management Wins

- **Proactive, not reactive** – risks managed from day zero.
- **Comprehensive coverage** – technical, process, and people risks included.
- **Playbooks in place** – no scrambling during incidents.
- **Board-ready reporting** – risk registers, heat maps, and RCA reports suitable for executive and audit committees.