Phase 3

Task 3.2: Risk Management and Contingency Planning

1. **Risk Register**

Risk Description	Probability	Impact	Mitigation Actions	Contingency Plan
Vendor License Expiration	High	High	Escalate to executive leadership; report to the CIO, while the CIO reports to the FiServ CEO. The legal team will review the contract.	If no response/key by midnight, the core banking system will be shut down and restarted.
Data Integrity remediation error	High	Medium	Senior QA will be assigned to lead the night shift to correct data errors manually	If the error persists, a full audit will be initiated, and the affected accounts will be isolated.
Wire Transfer Missing Deadline	High	High	Divert 2 staff to parallel recovery. Explore manual processing with a correspondent bank as a fallback.	If the deadline is missed, affected customers will be notified with a formal apology, also notify regulatory bodies.
Staff Fatigue/Burnout	High	Medium	Breaks will be mandated for staff; the shift will be initiated.	In case of an emergency, pull the staff off duty immediately and assign the task to the standby staff
ATM Instability	Medium	Medium	Implement a phased rollout	Disable unstable ATMs

2. **Go/No-Go Decision**

The decision to abandon the DR site will be made if the core banking system is unstable beyond 8:00 PM, the data that got corrupted due to the flood spreads beyond measure, if the vendor license is not resolved by midnight, or the DR infrastructure shows systemic failure. The alternative option may be to consider migrating to the cloud; the warm site can be pivoted to an emergency cloud service, such as Azure or AWS, leveraging cloud-based core banking system capability, which is faster and safer. Another option may be to contract a third-party data processor to handle core processing.