Enterprise Risk Register & Mitigation Plan

Project Meridian – Cloud Transition & Ledger Consolidation

Nexa Corporation • Finance & Risk Management Division

1 Executive Summary & Context

Project Meridian is a critical digital infrastructure transformation program undertaken by **Nexa Corporation** in partnership with **Synapse Systems Group**. The project aims to consolidate legacy financial transaction ledgers across five regional subsidiaries into a single cloud-native real-time ledger system, hosted on **Nimbus Infrastructure**.

As this project involves migrating high-value transaction processing pipeline systems, it carries significant operational, financial, compliance, and technical risks. This Risk Register serves as the definitive tool for tracking identified risk factors, assessing their raw impact, establishing ownership, and outlining mitigation workflows.

2 Risk Assessment Methodology

Risk severity is determined using a standard 5×5 matrix. For each risk, the probability of occurrence (Likelihood) and the severity of the consequence (Impact) are assigned a score from 1 to 5.

2.1 Likelihood Scale

- **1 – Rare:** Highly improbable; less than 5% chance of occurrence.
- **2 – Unlikely:** Possible but unexpected; 5% to 20% chance of occurrence.
- **3 – Possible:** Might occur at some point; 20% to 50% chance of occurrence.
- **4 – Likely:** Expected to occur; 50% to 80% chance of occurrence.
- **5 – Almost Certain:** Virtually guaranteed; greater than 80% chance of occurrence.

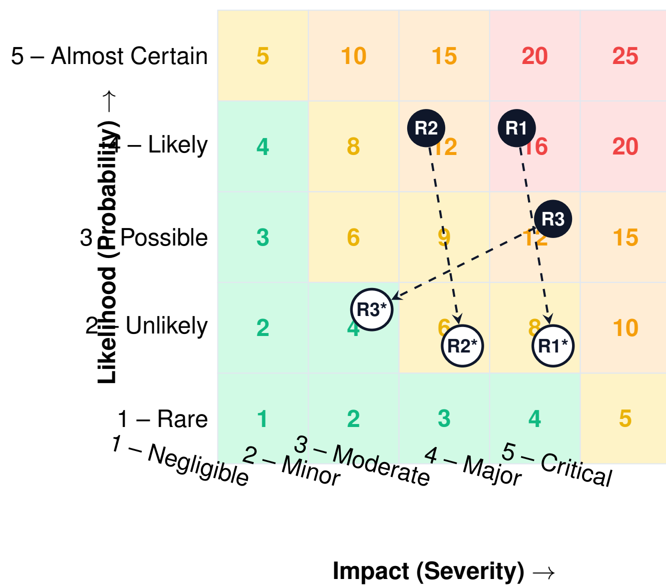
2.2 Impact Scale

- **1 – Negligible:** No financial impact; minor inconvenience to operations.
- **2 – Minor:** Financial loss under $50,000; localized delays of less than 2 days.

- **3 – Moderate:** Financial loss of $50,000 to $200,000; project delay of 1 to 2 weeks.
- **4 – Major:** Financial loss of $200,000 to $1M; critical milestone missed; external audit failure.
- **5 – Critical:** Financial loss exceeding $1M; project termination; systemic regulatory fines.

3 Risk Heatmap Matrix

The following 5×5 matrix illustrates the scoring system and highlights the active risk profile of Project Meridian before and after mitigation. The matrix colors denote the severity categories: **Low (1–4)**, **Medium (5–9)**, **High (10–15)**, and **Critical (16–25)**.



Risk Profile Summary

- **Total Identified Risks:** 5 key items across core domains.
- **Pre-Mitigation Profile:** 1 Critical, 2 High, 2 Medium.
- **Post-Mitigation Profile:** 0 Critical, 0 High, 3 Medium, 2 Low.
- **Key Focus Area:** Cross-border regulatory compliance and real-time synchronization throughput.

Mitigation Principles

All critical (red) and high (orange) risks require active mitigation controls and weekly status audits to the project board. Residual risk must be reduced below a score of 10 prior to production launch. Owner columns designate the single point of contact responsible for executing standard operating procedures (SOPs).

4 Project Risk Register

Below is the master Risk Register for Project Meridian. It outlines the raw risks, their primary response strategy, active mitigations, mitigation owners, and the resulting residual risk rating.

ID	Category	Risk Description	L_0	I_0	R_0	Mitigation Actions & Controls	Owner	L_r	I_r	R_r
R1	Compliance	**Regulatory Audit Failure:** Migrating subsidiary ledger systems violates local financial data sovereignty laws in secondary jurisdictions.	4	4	16	Establish localized database clusters within jurisdiction borders on Nimbus DB; employ automated compliance verification filters.	S. Vance (Compliance)	2	4	8
R2	Technical	**Data Sync Latency:** Intermittent API failures in Synapse ledger synchronizer cause transaction queue backups during peak hours.	4	3	12	Implement standard Kafka queues with dead-letter-queue retry mechanisms; scale API instances dynamically on Kubernetes.	J. Miller (IT Arch)	2	3	6
R3	Operational	**Key Staff Turnover:** Departure of senior data architects from Vertex Dev Team causes loss of critical custom ledger logic knowledge.	3	4	12	Implement strict documentation sprint goals; pair-program all integration modules; enforce 30-day knowledge handovers.	A. Patel (HR Lead)	2	2	4
R4	Financial	**Cloud Overspend:** Unoptimized dynamic query scaling on Nimbus Infrastructure leads to severe monthly billing overruns.	3	3	9	Define strict budget thresholds with auto-throttling; optimize indexing on heavy transaction tables; perform weekly query audits.	M. Chen (Finance)	2	2	4
R5	Security	**Data Exfiltration:** Insecure legacy database endpoints are targeted during the migration phase, compromising client transaction records.	2	5	10	Use Cloudflare Tunnels for secure migration channels; encrypt all data-at-rest using AES-256; enforce strict mutual TLS (mTLS).	L. O'Connor (SecOps)	1	5	5

5 Risk Response Strategies & Governance

Project Meridian risk management follows the frameworks established in the global corporate governance guidelines [1, 3]. Each identified risk must be categorized under one of the four corporate-approved risk response strategies:

Avoid: Alter the project scope, technical design, or deployment strategy to eliminate the risk entirely. This strategy is reserved for critical risks that cannot be mitigated cost-effectively.

Transfer: Delegate the risk to a third party. For example, using vendor-managed databases on **Nimbus Infrastructure** transfers server-level uptime risks to the cloud provider under a Service Level Agreement (SLA).

Mitigate: Implement operational, technical, or administrative controls to reduce either the Likelihood or Impact score (e.g., configuring Cloudflare Tunnels as detailed in [2]).

Accept: Maintain the current status without additional interventions. This is only permissible for low-level residual risks (score under 5) where mitigation costs exceed potential losses.

6 Escalation Workflow

The Steering Committee requires immediate escalation of any risk that experiences an upward rating trend during weekly status reviews. The following protocol defines escalation thresholds:

1. **Residual Risk Score 1–4 (Low):** Managed at the team level by the designated owner. Discussed in bi-weekly sprint reviews.
2. **Residual Risk Score 5–9 (Medium):** Monitored by the project manager. Requires monthly updates to the Program Management Office (PMO).
3. **Residual Risk Score 10–15 (High):** Requires direct approval of the Program Director. Mitigation plan status reviewed in weekly coordination meetings.
4. **Residual Risk Score 16–25 (Critical):** Demands immediate escalation to the Executive Steering Committee. The project may be suspended until a mitigation control is verified.

References

[1] International Organization for Standardization. Iso 31000:2018 risk management – guidelines. Standard ISO 31000, 2018.

[2] Sarah Jenkins. *Enterprise Integration Architecture: Scalable Solutions for Financial Services*. Meridian Technical Press, Apex City, 2023.

[3] Nexa Corporation Finance Division. *Enterprise Risk Management and Governance Manual*, 2024. Internal policy document ref: NX-RM-2024-V2.