

# Operational Risk Management SOP (OPS-RISK-001)

Department: Operations (Owned by COO)

Version: 1.0

Date: 2025-10-01

## 1. Scope and Objective

This SOP covers the identification, assessment, mitigation, and monitoring of non-financial and non-security **Operational Risks** that could disrupt NexaCore's ability to deliver its core SaaS platform or manage internal infrastructure effectively.

## 2. The Risk Management Cycle

NexaCore uses a standardized four-step cycle for continuous risk management:

### Step 1: Identification

- Method:** Quarterly Risk Workshops, Post-Mortems, and Departmental Audits.
- Documentation:** All risks must be logged in the **Operational Risk Register** with a unique ID (e.g., OPRISK-042).

### Step 2: Assessment (Impact vs. Likelihood)

Risks are scored on a scale of 1 to 5 for both **Likelihood** (1=Rare, 5=Almost Certain) and **Impact** (1=Minor, 5=Catastrophic).

| Total Score (L x I) | Risk Level        | Required Action   |
|---------------------|-------------------|---|
| 15 – 25             | Extreme (Red)     | Immediate action required.<br>Must be monitored weekly by Executive Team. |
| 8 – 14              | High (Amber)      | Mitigation plan must be assigned and actively managed quarterly.          |
| 4 – 7               | Moderate (Yellow) | Mitigation plan defined; monitored biannually.                            |
| 1 – 3               | Low (Green)       | Accept and monitor.   |

## Step 3: Mitigation Strategy (The 4 T's)

For all Extreme and High risks, one of the following mitigation strategies must be defined:

1. **Tolerate (Accept):** The risk is low or mitigation cost outweighs the potential impact.
2. **Treat (Mitigate):** Implement controls to reduce likelihood or impact (e.g., implement redundant ISP connections).
3. **Transfer (Insure):** Shift the risk to a third party (e.g., cyber insurance, outsourcing non-core functions).
4. **Terminate (Avoid):** Stop the activity that generates the risk (e.g., discontinuing support for an outdated, high-risk library).

## Step 4: Monitoring and Review

The Operations Team reviews the top 10 risks in the Register during the **Monthly Operations Review** meeting. Owners must provide a status update on their assigned mitigation tasks.

## 3. Sample Operational Risks (Focus: MENA & SaaS)

| Risk ID    | Risk Description   | Likelihood (L) | Impact (I) | Score (L x I) | Mitigation Strategy   | Owner         |
|------------|--|----------------|------------|---------------|---|---------------|
| OPRISK-021 | Critical personnel (Lead SRE) resignation resulting in loss of key infrastructure knowledge. | 3 (Possible)   | 4 (Major)  | 12 (High)     | Treat: Mandatory cross-training on 80% of infrastructure components; update documentation repository. | Head of Ops   |
| OPRISK-022 | Unexpected local regulator   | 4 (Likely)     | 4 (Major)  | 16 (Extreme)  | Treat: Legal/Compliance   | Legal Counsel |

|            |  |              |                  |              |   |                  |
|------------|--|--------------|------------------|--------------|---|------------------|
|            | Policy change regarding data transfer or sovereignty (e.g., KSA).                                |              |                  |              | to monitor local gazettes weekly; establish a regional Data Sovereignty Advisory Group.                 |                  |
| OPRISK-023 | Single-point failure in the Dubai HQ's secondary ISP resulting in loss of internal connectivity. | 3 (Possible) | 2 (Minor)        | 6 (Moderate) | Treat: Upgrade secondary ISP SLA to include 4G failover backup.   | Facility Manager |
| OPRISK-024 | Cloud vendor (AWS/GCP) service disruption in a key MENA region (e.g., Bahrain).                  | 2 (Unlikely) | 5 (Catastrophic) | 10 (High)    | Treat: Ensure geo-redundant backups are configured outside the primary regional cloud zone (BCDR Plan). | Head of SRE      |

