# Resilience Operations Center

## Protecting banking services availability by detecting disruptions before they impact customers.

For Indian banks, business continuity *is* the business. Millions of real-time transactions are processed every hour, and customers expect each one to go through the first time. An outage is no longer an IT incident — it is lost transactions, regulatory action, and a question for the board. The iStreet ROC brings IT operations, cybersecurity, fraud risk, and compliance into one AI-powered command layer, enabling banks to identify threats to operational continuity early and respond as one organisation.

**791 M**
UPI transactions a day in India — demand that never pauses

**$1.8 M**
Average cost of one hour of high-impact outage in financial services

**$152 M**
Average annual cost of downtime for a financial services organisation

**₹40.9 cr**
Average cost of a data breach for Indian financial services — highest of any sector

**6 hours**
Window to report a cyber incident to CERT-In

### Always-On Matters for Indian Banks

**Revenue at Risk.** Payments, cards, and digital lending run in real time. Every minute of unavailability is transactions and fee income that do not come back.

**Customer Attrition.**With UPI transactions and account opening now largely digital, a customer who can't transact can switch to a competitor the same day.

**Board Accountability.** Regulatory guidance on operational resilience, reporting timelines, and DPDP penalties makes continuity a board-level obligation.

**Siloed Risk Functions.** IT operations, cyber security, fraud, and compliance each monitor the bank through their own systems, and no single team sees how one event affects the others.

### What the ROC Delivers

**Continuity of Critical Operations.** Monitors core banking, UPI and IMPS, cards, ATMs, and internet and mobile banking end to end, predicting degradation before transactions fail.

**Business Impact Visibility.** Correlates infrastructure, application, security, and fraud signals, so teams know which customers and revenue lines are at stake.

**Integrated Cyber and Fraud Defence.** Detects attacks, suspicious activity, and fraud patterns in real time, and prioritises vulnerabilities by business risk.

**Recovery Within Tolerance.** Gives operations, security, and fraud teams one shared view and a coordinated response.

**Continuous Regulatory Compliance.** Captures every event and action as audit-ready evidence and supports reporting within regulatory timelines.

### ROC Solutions

| SOLUTION | WHAT IT DOES | BUSINESS OUTCOME |
|---|---|---|
| **AIOps** | Correlates infrastructure and application signals, predicts service degradation, and reduces alert noise | Higher availability of banking services; lower operational cost |
| **SIEM++** | AI-native security analytics across logs, users, applications, and infrastructure | Faster detection of cyber threats |
| **Unified Asset Visibility** | One inventory of every application, system, and device | No unmonitored assets; a clear view of exposure |
| **Governance, Risk, and Compliance** | Integrated, DPDP-aligned controls with automated evidence | Continuous regulatory readiness and board-ready reporting |
| **Sovereign AI Infrastructure** | On-premises, data-resident AI infrastructure built in India | Data stays in India; residency built into the architecture |

**iStreet Network Limited (BSE: 524622)** is a sovereign AI infrastructure and solutions provider for the world's most regulated sectors. Under the Sanjeevani of AI™ framework, its Resilience Operations Center brings AIOps, SIEM++, risk-based vulnerability management, unified asset visibility, GRC, and sovereign AI infrastructure into one connected framework — so critical banking services stay available, secure, and compliant around the clock.

ROOTED IN INDIA, ENGINEERED FOR THE WORLD

contact@istreetnetwork.com · istreetnetwork.com
4-A Wing, D J House, Old Nagardas Road, Andheri East, Mumbai 400069