HEAL AIOPS, POWERED BY ISTREET NETWORK · SOVEREIGN · ON-PREMISES

Unified Observability for Operational Resilience in Financial Services

Correlating every signal so service degradation is attributed before the customer feels it.

Operational resilience in banking rests on one capability: knowing, within minutes, which layer of a service chain is failing and which customers it reaches. That requires telemetry from every domain flowing into one correlated view, analysed inside the bank's own environment, and held there for as long as the regulator requires. Unified observability is the architecture that delivers it.

The data already exists. What is missing is correlation across it.

Four structural gaps in a tool-centric monitoring landscape

Visibility that stops at the domain boundary

Telemetry exists across servers, networks, applications, databases, and security systems, but each set is read in isolation. No continuous view spans a banking service end to end – from the customer channel through the API layer to the core and the database beneath it.

Alert volume without attribution

Every domain raises alerts. None of them answers the question that decides how long an outage lasts: is this the application, the database, the infrastructure, the network, the security layer, or a third-party dependency?

Compliance reconstructed for every audit

Log retention, immutability, evidence trails, and regulatory reporting are assembled after the fact rather than produced continuously by the monitoring architecture itself.

Data residency treated as a retrofit

Observability platforms designed for multi-tenant cloud delivery cannot be made data-resident by configuration. Sovereignty is an architectural decision, not a deployment option.

What operational resilience demands of a bank's monitoring architecture

One ingestion layer

Standardised collection of logs, metrics, traces, events, flows, and packet metadata across Data Centre and Disaster Recovery, from existing tools and new instrumentation alike.

Cross-domain correlation

AI/ML analysis that reduces alert volume through correlation, identifies probable root cause across layers, and ranks incidents by business and customer impact.

Sovereign deployment

Every signal, every derived analytic, and every model inference contained within bank-controlled infrastructure across DC and DR.

Open standards

OpenTelemetry-aligned collection and pipelines, so the institution retains the freedom to continue, integrate, replace, or add tools on its own terms.

Unified Observability - Built to the operating reality of Indian banking supervision

- **CERT-In Directions** – rolling 180-day log retention, maintained within Indian jurisdiction
- **Master Direction on IT Governance, Risk, Controls and Assurance Practices** – demonstrable monitoring, audit trails, and change and incident discipline
- **Cyber Security Framework and Digital Payments Security Controls** – continuous visibility across digital channels and payment rails
- **DPDP Act** – data residency and access governance designed into the architecture

THE FRAMEWORK

A layered observability architecture, built to run inside the bank.

The architecture is delivered on-premises across the Data Centre and Disaster Recovery with full parity, structured in five layers. Each layer works with the existing tools, rather than replacing them.

LAYER 1

Data Collection, including Network and Application Telemetry

- OpenTelemetry agents and instrumentation across servers, virtual machines, middleware, databases, the Core Banking System, payment systems, and digital channels
- Ingestion from existing monitoring, APM, and SIEM/SOC platforms through open APIs and connectors
- Ingestion of network telemetry – device metrics, interface statistics, link performance, flow records, and packet metadata – from existing or specialised Network Performance Monitoring and packet analytics tools
- DC and DR parity, so observability does not degrade during failover or scheduled DR drills

LAYER 2

Immutable Log Store and Ingestion

- On-premises telemetry and log repository within bank-controlled DC/DR infrastructure
- Retention aligned to the CERT-In 180-day minimum, with configurable retention, indexing, and archival policies by data class
- Centralised ingestion through OpenTelemetry Collector pipelines
- Indexing engineered for both real-time query and long-window historical investigation

LAYER 3

AI/ML Analytics Engine

- Behavioural baselining that reduces dependency on manual thresholds and static rules
- Anomaly detection across application, database, infrastructure, network, and log signals
- Automated root cause analysis across domains, and full causal chain, with event correlation and deduplication reducing alert volume ahead of it
- Business impact and customer experience impact assessment for critical banking services

LAYER 4

Integration and Automation

- ITSM integration for automatic incident creation, assignment, escalation, closure, and closed-loop remediation, linked to problem and change processes
- Bidirectional integration with SIEM and SOC platforms
- Automated runbooks and self-healing workflows
- Incident enrichment with topology, CMDB, service-impact, and business-impact context

LAYER 5

Unified Dashboards and Executive Information System

Role-based views, real-time and historical, with drill-down, filtering, correlation, export, and scheduled reporting under role-based access control and audit logging.

VIEW	DELIVERS
Executive and resilience	DC/DR resilience, MTTR trend, SLA and SLO status for core banking, UPI, and digital channels, regulatory compliance posture
IT and NOC operations	Active incidents, root cause and causal chain, ITSM queue status, capacity, DR readiness, SLA-breach countdown
Application and transaction	Application topology, transactions, financial and non-financial transactions, success and failure rates, API and database performance
Infrastructure and network	Compute, memory, storage, disk I/O, VM and container health, bandwidth, interface errors, capacity trend
Security, compliance, and audit	Security event volumes, failed authentication, vulnerability posture, audit trails, log-retention compliance

OUTCOMES

Application performance, discovery, and service management

The framework delivers the same result whether a tool is continued, integrated, or replaced. It collects telemetry from every source, correlates it, and presents it in a single-pane-of-glass view, regardless of which tool generated it. The sections below set out what that means for application performance, infrastructure, and service management.

Application Performance Monitoring

APM covers end user experience, architecture discovery, transaction profiling, deep-dive diagnostics, and analytics across core banking, Internet and Mobile Banking, UPI, IMPS, NEFT and RTGS, AEPS, API gateways, and lending and cards – delivered natively where an existing APM tool is correlated.

- Performance, availability, response time, throughput, error rate, transaction latency, failed transactions, application logs, errors, and exceptions
- API availability, response time, latency, error rate, and service degradation
- End user experience monitoring across digital channels, with synthetic monitoring and reporting
- Automatic discovery and modelling of application architecture, service dependencies, APIs, databases, middleware, and supporting infrastructure
- Continuous topology mapping in Business View and Technical View, with SLOs linked to end-to-end transaction traces
- AI/ML anomaly detection, correlation, and automated RCA across application, infrastructure, and database layers

Infrastructure monitoring, discovery, topology, and service management

- Infrastructure monitoring across servers, operating systems, virtual machines, middleware, application servers, and enterprise IT components
- Application health, availability, utilisation, performance, capacity, events, and service-impacting condition detection
- AIOps correlation, deduplication, noise reduction, anomaly detection, probable root cause, and business-impact-based prioritisation
- Discovery across infrastructure, applications, network components, middleware, databases, and service dependencies in DC, DR, and near-DR environments
- Automatic topology mapping, service modelling, and relationship mapping to business services
- ITSM integration across the full incident lifecycle

Deployment and Data Residency

Sovereign by design and architecture. Deployed entirely within the bank's own Data Centre and Disaster Recovery environment. All observability data – logs, metrics, traces, events, alerts, topology, configuration, packet metadata, flow records, application performance data, user experience data, incident records, and derived analytics – resides within bank-controlled infrastructure.

Outcomes

- Unified observability across infrastructure, network, application, database, and security domains
- Faster attribution of whether degradation originates in the application, database, infrastructure, network, security layer, or a third-party dependency
- Continuous, provable compliance with RBI and CERT-In requirements
- Reduced MTTR and reduced alert volume through correlation rather than filtering
- Predictive operations through AI/ML baselining rather than static thresholds
- Freedom to rationalise, continue, integrate, or replace existing tools on the institution's own timeline

iStreet Network

Modernization, security, governance, and operations are usually bought separately. That separation is what leaves telemetry disconnected, compliance reconstructed, and residency retrofitted.

iStreet Network Limited is an enterprise-grade, sovereign AI ecosystem. At its core is Sanjeevani of AI™ – iStreet's AI Centre of Excellence and integrated framework, bringing observability, security, governance, risk, and compliance together as one connected architecture. Unified observability is where that architecture meets daily banking operations, and the Resilience Operating Centre is where it runs.

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