# 9. Tracking, Monitoring, and Audit

## 9.1 The Importance of Visibility

In a clearance regime like FIRS MBS, compliance does not end when an invoice is submitted. Enterprises must be able to **prove** that every invoice was submitted, cleared, and archived, while also detecting issues in real time. Softrust and Bluelight provide unified tracking and monitoring that gives Finance, IT, and Compliance stakeholders confidence at all times.

<diagram: Three-pane dashboard — Finance (status), IT (infrastructure), Compliance (audit evidence)>

---

## 9.2 Real-Time Tracking

- **Status Views** – every invoice visible from submission through clearance or rejection.
- **Search and Filter** – by invoice number, TIN, clearance ID, company code, or date range.
- **Drill-Downs** – see full payload, response, and evidence bundle per invoice.
- **Correlation IDs** – unique identifiers link SAP/ERP entries to FIRS receipts, ensuring traceability.

---

## 9.3 Monitoring for IT Teams

- **Platform Metrics** – throughput, latency, error rates, queue sizes.
- **Alerting** – configurable thresholds for SLA breaches (e.g., clearance delay > 30 min).
- **Infrastructure Health** – CPU, memory, and certificate expiry alerts.
- **Integration Monitoring** – webhooks, callbacks, and SFTP channels monitored with retries and alerts.

<diagram: IT monitoring dashboard showing latency graphs, error spikes, and alert indicators>

---

## 9.4 Compliance Dashboards

- **Clearance Rates** – percentage cleared vs submitted in real time.
- **Rejection Reasons** – categorized by missing TINs, tax codes, HS codes, or formatting issues.
- **Reconciliation Reports** – SAP vs SmartAPI vs FIRS counts, with exception queues.

- **Audit Trails** – logs of who submitted, when, what response was received, and how corrections were handled.

---

# 9.5 Evidence Bundles

Every cleared invoice generates a **complete audit package**, including:

- Canonical JSON payload
- Signed submission file
- Clearance receipt from FIRS (IRN, QR, timestamp)
- PKI digital signature for integrity
- QR code image for verification
- Audit log extract with all events and correlation IDs

These bundles are **immutable** and stored in WORM (Write Once, Read Many) archives for a minimum of 10 years.

---

# 9.6 Daily and Intraday Reconciliation

- **Daily Jobs** – reconcile invoice counts across ERP, SmartAPI, and FIRS.
- **Intraday Spot Checks** – random checks on high-value invoices.
- **Exception Queues** – flagged mismatches reviewed by Finance before day end.
- **Signed Reports** – reconciliation reports digitally signed and stored alongside evidence bundles.

<diagram: Reconciliation flow — ERP totals vs SmartAPI vs FIRS → exception queue → signed report>

---

# 9.7 Alerting and Notifications

- **Finance Alerts** – invoice rejected, immediate email or dashboard alert.
- **Compliance Alerts** – daily reconciliation mismatches.
- **IT Alerts** – integration or infrastructure errors, certificate expiry, queue backlogs.
- **Custom Channels** – alerts can be pushed into ServiceNow, Jira, or Microsoft Teams.

---

# 9.8 Audit Readiness

- **One-Click Retrieval** – auditors can request evidence for any invoice via dashboard or API.
- **Bulk Export** – monthly or quarterly ZIP bundles for external regulators.
- **Immutable Logs** – all submissions, responses, and corrections preserved.
- **Proactive Audits** – quarterly mock audits performed jointly with client Compliance teams.

---

## 9.9 Why This Matters to the Client

- **Finance Teams** get real-time visibility and assurance that invoices are cleared.
- **IT Teams** get dashboards, alerts, and control over integration health.
- **Compliance and Audit** get legally defensible evidence with zero effort.

Together, these capabilities transform compliance from a **risk exposure** into a **controlled and monitored process**.