CASE STUDY

IBM i Audit Trail Integrity with AP-Journal & Change Tracker

European Financial Institution *Anonymized | Confidential*

Client Profile

Industry	Financial Services
Region	Europe
Environment	IBM i — 6 LPARs supporting core banking, payment processing, customer account management, lending operations, and regulatory reporting
Security Scope	Database Activity Monitoring, Change Management, Audit Trail Integrity, and Compliance Reporting
Assessment Type	Regulatory Compliance & Internal Security Governance Initiative

The Challenge

The financial institution managed large volumes of sensitive customer, transactional, and financial data on IBM i systems. Regulatory requirements and internal governance policies demanded comprehensive visibility into database modifications and system changes affecting critical business operations.

Limited Visibility into Database Activity

While journaling mechanisms were available within IBM i, security and audit teams faced challenges obtaining meaningful insight into database transactions and record modifications. Concerns included:

- Difficulty identifying who modified sensitive customer and financial records
- Limited visibility into before-and-after values of critical transactions
- Time-consuming analysis of journal information during audits
- Delayed investigations into suspicious activity
- Lack of centralized reporting for compliance reviews

The organization required a solution capable of transforming IBM i journal data into actionable security and audit intelligence.

Insufficient Control Over System Changes

The institution also needed greater oversight of modifications affecting IBM i system configuration, security settings, and critical objects. Challenges included:

- Difficulty tracking unauthorized configuration changes
- Limited accountability for modifications to system values and security-related settings
- Increased effort required for compliance reporting
- Challenges validating change management procedures
- Need for improved visibility in administrative activities

Security and compliance teams sought a comprehensive approach to monitor both database activity and system-level changes.

Solution Deployed

Raz-Lee deployed the following iSecurity modules across the IBM i environment:

iSecurity AP-Journal

Implemented advanced monitoring and analysis of IBM i journal activity. Capabilities included:

- Real-time monitoring of journalized database transactions
- Tracking of record additions, modifications, and deletions
- Detailed before-and-after value reporting
- User-level accountability for database changes
- Centralized reporting and search capabilities
- Accelerated audit and forensic investigations

iSecurity Change Tracker

Implemented continuous monitoring of changes affecting IBM i system security and configuration, like:

- Monitoring of system values and security settings
- Tracking changes to user profiles and authorities
- Detection of modifications to critical system objects
- Automated recording of administrative activities
- Detailed audit trails supporting compliance requirements, configuration and security changes

Together, AP-Journal and Change Tracker delivered comprehensive monitoring of both business data and IBM i system changes.

Results

- Improved visibility into database and system-level activities
- Strengthened accountability for sensitive data modifications
- Enhanced monitoring of configuration and security changes
- Accelerated audit preparation and regulatory reporting
- Reduced investigation time for suspicious or unauthorized activities
- Improved validation of internal change management procedures
- Deployment completed without disruption to critical banking operations

The organization achieved a significantly higher level of visibility, control, and audit readiness across its IBM i environment.

Key QSA Feedback

> *"Financial institutions must demonstrate complete traceability of both data changes and administrative actions. By combining AP-Journal and Change Tracker, we gained the visibility needed to satisfy auditors, strengthen change management controls, and quickly investigate any activity affecting our IBM i environment."*

— Head of IT Security & Compliance (paraphrased)