CASE STUDY

IBM i Privileges - Authority Inspector & Authority on Demand

International Banking Group *Anonymized | Confidential*

Client Profile

Industry	Banking & Financial Services
Region	Europe
Environment	IBM i — 8 LPARs supporting core banking, payment processing, treasury operations, customer account management, SWIFT connectivity, and regulatory reporting
Security Scope	Privileged Access Management, Authority Governance, Segregation of Duties, and Compliance Monitoring
Assessment Type	Access Control & Regulatory Compliance Initiative

The Challenge

The banking group operated a complex IBM i environment supporting critical financial services across multiple countries. Regulatory requirements and internal security policies demanded strict control over privileged access while ensuring administrators could perform operational tasks when necessary.

Excessive User Privileges

Over time, many users accumulated authorities that exceeded their day-to-day responsibilities.

- Excessive access to sensitive banking applications and data
- Difficulty identifying users with elevated privileges
- Increased risk of insider threats and unauthorized activities
- Challenges enforcing least-privilege principles
- Limited visibility into authority inheritance and special authorities

The organization required a comprehensive review of user permissions and a strategy to reduce unnecessary privileges.

Permanent Administrative Access

Administrators and support personnel maintained continuous access to highly privileged functions, creating compliance and security concerns. Challenges included:

- Standing privileged access increasing risk exposure
- Difficulty enforcing temporary administrative access
- Limited accountability for elevated authority usage
- Increased auditor scrutiny of privileged accounts
- Need for stronger segregation of duties controls

The bank sought a solution capable of reducing permanent privileges while maintaining operational efficiency for IT teams.

Solution Deployed

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

iSecurity Authority Inspector

Implemented advanced authority analysis and privilege assessment capabilities. Capabilities included:

- Identification of excessive and inherited authorities. By user, group, and object permissions
- Discovery of privilege escalation risks
- Visibility into special authorities and security exposures
- Support for least-privilege initiatives
- Detailed reporting for auditors and compliance teams

The solution enabled the organization to identify and remediate unnecessary privileges across the IBM i environment.

iSecurity Authority on Demand

Implemented controlled and temporary elevation of privileges for authorized users. Including:

- Automatic expiration of elevated privileges
- Approval-based authority assignment workflows
- Detailed auditing of privilege requests and usage

The implementation ensured that elevated access was granted only when required and only for the duration necessary to complete authorized tasks.

Results

- Reduced excessive privileges across IBM i systems
- Strengthened enforcement of least-privilege principles
- Eliminated unnecessary standing administrative access
- Improved segregation of duties and access governance
- Enhanced visibility into privileged user activities
- Increased compliance with banking regulations and audit requirements
- Reduced risk associated with insider threats and privileged account misuse
- Deployment completed without disruption to banking operations
- The organization significantly improved its privileged access management framework while reducing security risks and strengthening regulatory compliance across its IBM i environment.

Key QSA Feedback

> *"Managing privileged access in a banking environment requires balancing operational efficiency with strict security controls. Authority Inspector provided the visibility needed to identify excessive privileges, while Authority on Demand allowed us to eliminate standing administrative access and adopt a true least-privilege model. The result was stronger security and a much smoother audit process."*

— Chief Information Security Officer (paraphrased)