

CASE STUDY

IBM i Compliance Automation & Security Governance

European Wholesale Distribution Company *Anonymized | Confidential*



Client Profile

Industry	Wholesale Distribution
Region	Europe
Environment	IBM i — 5 LPARs supporting ERP, warehouse management, procurement, logistics, finance, and customer operations
Security Scope	Compliance Management, Security Configuration Control, Risk Assessment, and Audit Readiness
Assessment Type	Regulatory Compliance & Internal Security Governance Initiative

The Challenge

The wholesale distributor relied on IBM i as a critical platform for managing inventory, supply chain operations, customer transactions, and financial processes. As the company expanded across multiple European markets, compliance requirements and internal security standards became increasingly difficult to manage consistently.

Complex Compliance Requirements

The organization was required to demonstrate adherence to multiple internal policies and external regulatory frameworks. Challenges included:

- Difficulty validating IBM i security configurations against corporate standards
- Time-consuming manual compliance assessments
- Limited visibility into security weaknesses and configuration gaps
- Inconsistent compliance reporting across multiple IBM i environments
- Increased effort required to prepare for audits

The IT and compliance teams required a more automated approach to evaluating and maintaining compliance.

Lack of Continuous Security Governance

Insurance Security administrators needed better oversight of critical system controls to ensure compliance was maintained over time. Concerns included:

- Unauthorized changes to security-related system settings
- Configuration drift between IBM i partitions
- Difficulty tracking remediation activities
- Limited ability to demonstrate ongoing compliance
- Increased risk of audit findings and security gaps

The organization sought a centralized solution capable of continuously monitoring, evaluating, and managing IBM i compliance requirements.

Solution Deployed

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

iSecurity Compliance Evaluator

Implemented automated compliance assessment capabilities for IBM i.

iSecurity Compliance Manager

Implemented centralized compliance management and remediation tracking.

iSecurity System Control

Implemented continuous monitoring and control of critical IBM i security settings.

Together, these solutions provided a comprehensive framework for maintaining compliance and strengthening security governance across the IBM i environment.

Including:

- Continuous compliance monitoring
- Detailed compliance scoring and reporting
- Accelerated audit preparation processes
- Monitoring of security-sensitive system values
- Detection of configuration deviations
- Identification of policy violations
- Strengthened governance of IBM i security controls

Results

- Reduced time required for compliance assessments and audit preparation
- Improved visibility into IBM i security posture across all LPARs
- Accelerated identification and remediation of compliance gaps
- Strengthened governance of security-related system configurations
- Improved consistency of security controls across the environment
- Enhanced reporting capabilities for auditors and management
- Reduced operational effort associated with compliance management
- Deployment completed without disruption to warehouse, logistics, or ERP operations

The organization significantly improved its ability to maintain regulatory compliance, enforce security policies, and demonstrate continuous governance across its IBM i infrastructure.

Key QSA Feedback

“Maintaining compliance across multiple IBM i systems was becoming increasingly resource-intensive. Compliance Evaluator, System Control, and Compliance Manager gave us the visibility, automation, and governance capabilities necessary to continuously assess our security posture and dramatically simplify audit preparation.”

— IT Governance & Compliance Director (paraphrased)