

QJRN/400

A COMPREHENSIVE AUDITING PLATFORM FOR THE System i



Your IT data are major assets.

Be sure to protect,
monitor,
control their evolution,
and ensure their confidentiality
and relevance...

COMPLIANCE

International regulations including SOX, HIPAA, BASEL II, PCI, 21-CFR increasingly demand that firms maintain the security and integrity of Corporate Data.

FRAUD, SABOTAGE AND DISCLOSURE

60% of malicious acts are perpetrated by internal elements in a company.
In most cases these acts go undetected.

INTERNAL AUDIT

ISO 17799 establishes strict guidelines in terms of legal conformity, control audits, and internal controls.

Auditors today, are requiring companies to demonstrate and validate their level of conformity.

AUTOMATING THE PROCESS OF COMPLIANCY

Maintaining compliance is a costly endeavour for companies.
QJRN/400 can significantly reduce the number of man-days required for supporting the compliance program by automating the process of monitoring and reporting on all critical events.

Legislations concerning internal control

(Sarbanes-Oxley, HIPAA, Basel II, C-198, PCI, 21-CFR, laws against money laundering, ...) are getting tougher and hold directors and administrators of financial organizations and quoted companies directly and criminally responsible if they have not set up a structure for securing and auditing their information system.

The QJRN/400 and CONTROLER Security Suite

offers you a comprehensive solution to fulfil these audit requirements.

Complete Deployment in Days, not weeks!

QJRN/400

THE Audit Solution for IBM System i

SYSTEM AUDIT

The System Audit module meets all your audit requirements in terms of security, connection attempts, configuring system values, libraries and objects:

- Monitor sensitive profiles (remote maintenance, service providers)
- Audit actions carried out on confidential spool files, etc
- Interventions on profiles, system values, network attributes, authorization on sensitive objects
- Attempts to open a session or access unauthorized resources
- Monitor activity outside office hours
- Integrity check on audit parameters
- Monitor control transfers to production.

DATABASE AUDIT

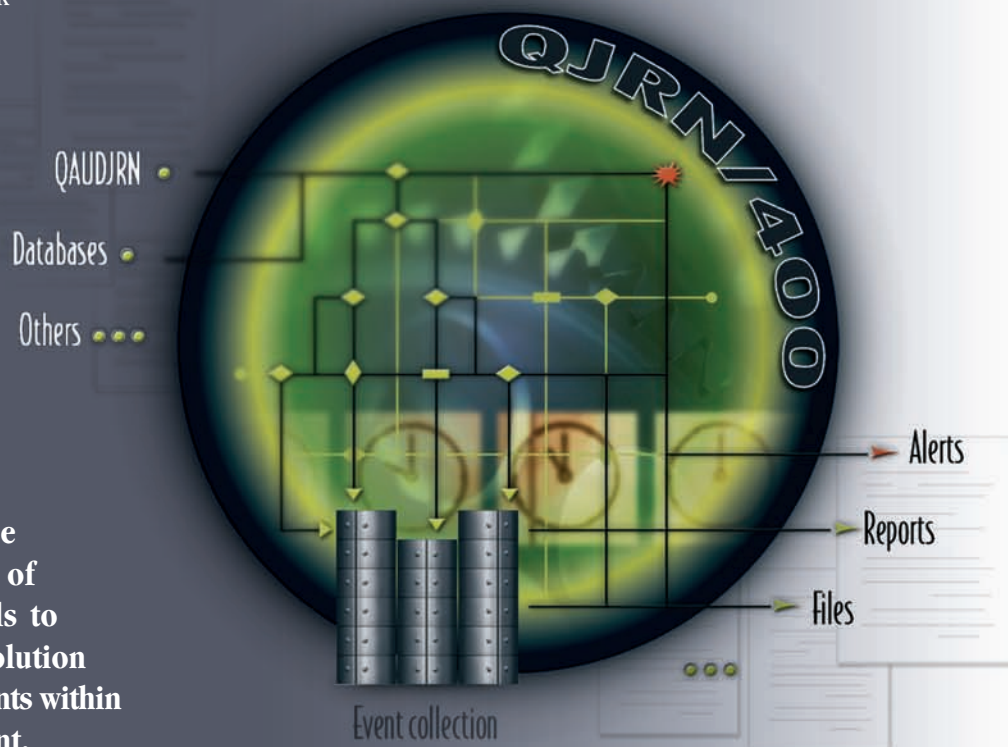
The Database Audit Module provides in depth, clearly detailed reports regarding modifications made to any database file anywhere on your system.

Easily flag and report on:

- Changes to Authorization Files
- Abnormal Changes to Credit Limits
- Activity Directed to Dormant Bank Accounts
- Inappropriate Changes To User Profiles
- Interventions on Sensitive Fields (Bank Account Number, Credit Cards, Account Limits)
- Operations made outside of an application: i.e., DFU, SQL
- Modifications made remotely to corporate applications through "in-house" or Third Party Programs.

QJRN/400 provides the appropriate combination of audit and security controls to help companies build a solution for managing all critical events within any production environment.

Operation	Date	Time	Job	User	Profile	TYP	Status	PGM	PNO	PEX	ALL	JOB	NAV	SEC	SPL	SRV	AUD	SQA	Source
User Profile	05/01/2007	14:05:09	QPADEV004	ADMIN	ADMIN	CHG	ENABLED	Y											
User Profile	05/01/2007	14:37:51	QPADEV004	ADMIN	OLASORT	CRT	ENABLED	Y	Y										
User Profile	05/01/2007	15:01:33	QPADEV004	ADMIN	OLASORT	CHG	ENABLED				Y								
User Profile	05/01/2007	15:19:19	SEC_CONSOL	ADMIN	USER_IDE	CHG	ENABLED												ADMIN
User Profile	05/01/2007	15:19:47	SEC_CONSOL	ADMIN	USER_IDE	CHG	ENABLED				Y	Y							Y
User Profile	05/01/2007	16:16:40	TD1001	ADMIN	QSEC_TMP	CRT	ENABLED		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
User Profile	05/01/2007	16:30:06	TD1001	ADMIN	QSEC_TMP	CHG	DISABLED												
Delete	05/01/2007	16:47:22	TD1001	ADMIN	QSEC_TMP														



MAIN FEATURES

Journaling Administration

All journals (system, database, or user-defined) can be declared and monitored by QJRN/400. Features include the ability to create new journals and easily register existing journals.

Each environment has a repository that describes the fields in the fully journaled database. This repository is automatically generated, and offers an almost unlimited possibility for customization.

Complete Compatibility With HA Platforms

QJRN/400 has been successfully integrated with the main HA solutions developed for the System i.

Query Manager

Incorporating a unique and original concept of Query Systems, QJRN/400 brings a level of business intelligence to the journaling process. The contents of individual receivers are queried for specific, user defined, events and/or syntax that could potentially indicate fraudulent activity or inappropriate access to sensitive data. The ability to customize these queries for specific databases, files, or fields allows companies to present the content of receivers in a clear, readable, and completely understandable format.

Automating The Audit Process

In addition to giving companies the ability to capture an almost unlimited range of data and events, the Query Manager incorporates a highly customizable reporting engine. Simple OS/400 messages or e-mails can be automatically generated and triggered by individual events or alarms. Daily, weekly, hourly printed reports, PDF files or e-mails can be output and delivered to the appropriate departments.

SELECTION OF SENSITIVE INFORMATION

QJRN/400 can identify "Concept Sensitive" Events that are potentially fraudulent.

- System i Administrators have numerous selection possibilities with standard operators (=, >, <, Like, Range, List...) or by specific programs applicable on all fields, as absolute value or by variation (by value, percentage or specific to dates).
- The lists of values to select or omit can be entered or filled by a program or a previous query.
- Generic selections such as "operations carried out outside business hours" or "operations carried out outside application" (by comparison to a program repository).
- Selections on relative numbers, profiles (class, group, special authority), programs, jobs, systems, or periods.

THE DIFFERENT PROCESSING MODES

Built-in flexibility for developing a real time security solution.

- **Query On-Demand Mode:** queries can be run interactively or in batch mode. This mode is used by administrators to retrieve immediate status reports, or to help isolate the source of malicious events or fraudulent activity.
- **Continuous Mode:** Query Manager can run continuously to monitor and detect patterns or trends that may be indicative of fraudulent behaviour. This Continuous Mode can also be used to detect anomalies or software bugs that trigger specific events. An alert can be sent to the appropriate person upon the appearance of the event being monitored.
- **Automatic Mode:** automatically set off when receivers are detached. This mode ensures the collection of data is exhaustive, whether these are for statistics or trace-ability in the case of quality monitoring.
- **Scheduled Mode:** extracts historical information of your application or system over a user defined period (year, month, day, hour, minute).

MULTIPLE REPORTING TOOLS & FORMATS

Regardless of the mode administrators use to extract data, QJRN/400 offers a broad range of output formats – PDF, EXCEL, WORD – using communication protocols such as FTP and SMTP.

From a single event to months of activity, department personnel can quickly create reports to meet both internal and external audit requirements.

- **Event & Trend Reports:** ability to capture a fixed image of a single entry to a receiver or a summary of a number of events to help identify user activity and trends.
- **Triggered Event Reports:** typically an e-mail alert triggered as a result of suspicious activity that requires immediate attention (i.e. credit limit changed for customer or vendor).
- **Trace File Reports:** this is a compressed summary of the history log containing only critical or relevant events. Capturing selective events rather than everything from the journal significantly reduces on line storage requirements, and allows to better exploit the reports.
- **Preparation File Outputs:** for large volumes, these allow you to carry out a pre-selection that can be used by one or more other queries.

Remote Replication

QJRN/400 includes a replication feature to allow companies to remotely deploy identical queries and reporting models. This capability allows the central IT department to build a consistent security process and policy to remote offices without the need to recreate the business rules again from scratch.



STANDARD FEATURES

- Virtually unlimited scalability to allow companies to audit all vulnerable points
- Multiple Reporting Formats
- Unique event extraction process ensures absolute data integrity
- Ability to isolate "critical" events minimizes the size and complexity of reports
- Real time alarms allow management to quickly react to critical events
- Report Builder allows non-IT staff to easily create independent reports for auditors and management
- Platform includes both Database and System Audit modules
- Ability to create a centralized audit scheme and quickly distribute to remote sites
- Standard Audit templates to facilitate easy deployment



ADDED VALUE

- Additional Level of security lowering the risk of fraudulent activity
- Audit features help to minimize potential financial losses and litigation problems
- Highly automated, QJRN/400 audits your system 24 hours a day, 7 days a week
- Tightly integrated with most HA platforms
- Rapid return on investment by reducing the on-going cost of compliancy



QJRN/400 and CONTROLER

are products designed and developed by



Z.I. des Iles • 190, route des Sarves
74370 METZ TESSY
FRANCE
Tel.: +33 4 50 69 45 98
Fax: +33 4 50 69 45 99
Email: contact@cilasoft.com
Web: <http://www.cilasoft.com>

ACCESS CONTROL

QJRN/400 can be integrated with our **CONTROLER** software to build **a complete audit and security solution:** a single platform for managing user access and detailed monitoring of all events.



**THE SATISFACTION OF KNOWING
WHAT'S GOING ON INSIDE!**

YOUR CONTACT