AUDIT MANAGER

ANALYZE ACCESS AND IMPLEMENT SEGREGATION OF DUTIES: CONTROL YOUR KEY FRAUD RISKS

HOW SECURE IS YOUR SYSTEM?

Whether your main concern is to prevent fraudulent activity or to satisfy the demands of your auditors, the ability to enforce and sustain effective Segregation of Duties (SoD) controls is an important tool to have in your kitbag.

Unfortunately, native JD Edwards EnterpriseOne contains no functionality to help you manage SoD or to facilitate compliance reporting. Many people try to manage it using spreadsheets and manual checks, but as well as being cumbersome and time-consuming, this approach is unreliable. Spreadsheets are notoriously prone to error; it is difficult to enforce version control; and any changes made within spreadsheets can't be audited.

INTEGRATED SOD MANAGEMENT

Audit Manager enables you to maintain an SoD model within your JD Edwards EnterpriseOne environment and run regular checks to identify users who have access permissions that would enable them to violate your SoD policy. Where SoD conflicts are found, you can drill down to investigate and remediate the issues, or, if appropriate, apply fully documented mitigating controls.

HOW IT WORKS

AUDIT MANAGER COMPRISES:

- Custom programs and tables held within your JD Edwards environment, which enable you to maintain your SoD rules
- A starter SoD model of the "Critical Risk" rules, as recommended by leading auditors, which you can adapt or extend to reflect your own SoD policy
- A powerful scanning engine that analyzes your live F00950 security table and stores the results in custom tables
- A set of standard enquiries and reports
- With results all stored in tables within your JD Edwards environment, you can also create your own reports using Insight Reporting for Q Software or your preferred third party reporting solution

BENEFITS

- Automated Segregation of Duties management saves times and improves accuracy
- Reduces the risk of fraud or costly error due to inappropriate access
- Pre-seeded rules speed up the implementation process
- Mitigating controls eliminate many false positives
- Speedy access to the information you and your auditors need
- Helps you keep your system in good shape and reduces the time needed to prepare for audits

MAIN FEATURES

INTEGRATED WITHIN YOUR JD EDWARDS ENVIRONMENT

All the processes and files used and produced by Audit Manager are held securely within your ERP environment, which has important benefits:

- Access to the SoD rules maintenance programs and the rules themselves can be restricted to authorized users
- Any changes made are fully auditable
- The SoD rules and the analysis results produced by the scanning engine are stored as custom tables and can be reported upon using our tools or your preferred reporting solution
- There's never a need to search for the right spreadsheet or worry about version control

So you can be confident in the knowledge that your reports are always based on accurate, current information rather than exported spreadsheets.

FOUR TYPES OF SOD RULES

We recognize that organizations differ widely in their compliance needs. Audit Manager offers four different types of rules so that your controls can be as granular as needed to satisfy your auditors' specific requirements:

Role level

The highest level of rule allows you to stipulate that specified Role combinations should not be assigned to the same user.

Duty level

Allows you to group a number of programs together as a Duty and then define rules stipulating that specified combinations of Duties should not be assigned to the same user (for example Sales Order Entry / Purchase Order entry).

Object level

Allows you to specify individual programs that should always be segregated.

Critical Object

This type of rules allows you to monitor access to Critical Objects - high risk programs which, even used in their own right, enable a user to commit fraud (for example access to the Bank Account or Next Numbers).
When used in conjunction with Security Manager Pro or Security Manager Express, the SoD Rules can be used to check proactively for conflicts before they are built into your live security.

PRE-SEEDED RULES

To help speed up implementation, we supply pre-seeded Segregation of Duties Rules, as recommended by leading auditors, which you can adapt or extend to reflect your own SoD policy.

FULLY DOCUMENTED MITIGATIONS

To cater for circumstances where you need to grant permissions that contravene your SoD policy, for example when staff need to take on extra responsibilities to cover for vacation, sickness or other temporary absence, Audit Manager allows you to apply Mitigations with effective start and end dates. Current mitigations will be taken into account when you run SoD analyses, reducing the occurrence of false positives and time wasted investigating them.
The details of mitigations are documented so that you and your auditor can see who applied them, why and how long they were in place.

ENQUIRIES AND REPORTS

With native JD Edwards EnterpriseOne, it takes a lot more effort than it should to answer such questions as:

- Who can access a give program and with what authorities?
- What programs can a particular user access and how do they get there?

Audit Manager includes 24 standard reports to deliver fast answers to the common questions that auditors ask. For example, our Application Security Net Effect and Row Security Net Effect enquiries enable you to quickly find out whether a user can access particular applications or data items, and at what level the prevailing security is held.
They display the applicable security settings at all levels (ie *Public, Role and User) and calculate the Net Effect to show you whether the User can access the specified item or not.
Where more flexible or customized reporting is needed, you can create your own reports using Insight Reporting for Q Software or your preferred third party reporting solution.
You can keep historical analyses as well as current ones, allowing you to monitor trends over time to monitor improvements or detect an increase in violations that may need investigating.