Segregation of Duties to Comply with Sarbanes-Oxley Requirements

By Laura Jackson

Editor's Note: Laura Jackson reports on her recent engagement with Hamilton Sundstrand to identify employees who have access to programs that create a potential conflict of interest. For example, an employee should not be able to enter a voucher and cut a check. This covered Financials, Distribution/Logistics, and Manufacturing, and used a combination of technical and non-technical methods of discovery and analysis. Hamilton Sundstrand agreed to let Laura share the discovery process with our readers.

What are we talking about when we refer to Segregation of Duties? Sarbanes-Oxley (SOX) mandates that there be certain controls within a company and the company's software. For example an employee should not be able to update the Supplier Master and Receive goods or services. The objective of this project was to confirm that appropriate controls are in place; we needed a way to identify employees who have access to programs that create potential conflicts of interest.

Start with how the users' security profiles are set up; that is, instead of individual access we use group profiles. This is easier to maintain and control as employees change positions or their authorization levels change. For example, security for all JD Edwards EnterpriseOne® users can be determined by the users' normal day-to-day functions. Those who perform similar systems tasks can be classified into the same User Group. Each such user group will then have its own security requirements. For example, the Accounts Receivable system could be divided into three user groups (manager, supervisor, and data entry groups), each of which performs different system tasks and requires different access authorities. It also helps to have a standard naming convention for both users and groups.

Menu security is not addressed in this article, but should be a part of your evaluation and analysis. We've always used menu security to restrict access to certain applications. With users and applications becoming more sophisticated, menu security is not enough. Keep in mind about your Portal and Web access programs.

Segregation of duties can be a complex equation involving many variables, but when you break them down into their simplest elements, the formula becomes pretty straightforward. Develop questions that identify three classes of job duties:

1. Authorization
2. Custody of Assets
3. Recording of Transactions

Once a question is identified as being in one of these three classes, the questions that fit into the other two classes must be reviewed. If the same user ID appears in more than one of these three classes, the user should be put into a table identifying them as a potential conflict of interest.

We should also address these questions not only within JDE software, but all software that interfaces with JDE, such as General Ledger, Pricing, Transportation software, etc. This is the case of companies that use Third-party software that could be tailored to their business.

This is not only about JD Edwards EnterpriseOne software, but also about your company's systems as a whole. When building your questionnaires remember all aspects of your system, for example:

Copyright© 2005 Klee Associates, Inc.

Revenue and Receivables

- Customer Orders/Initial Approvals
- Shipments & Physical Control of Finished Goods
- Cash Receipts/Record Maintenance

Purchasing and Payables

- Establishment of Disbursement Support
- Cash – Limit Access and Verify Existence
- Accountability (including detection of unauthorized entries)

Production

- Approvals of Production Requirements
    - Cost Factor
    - Work Center Rates
    - Frozen Update Program
- Maintains Unit Perpetual Records

EnterpriseOne system administrators can use the tools built within the software in order to analyze and secure your company's systems. For example, EnterpriseOne uses the Security Workbench table (F00950), to control security for individual users and for groups of users.

EnterpriseOne security is at the object level. This means that you can secure specific objects, which provides flexibility and integrity for security. For example, you can secure a user from a specific form, and no matter how the user tries to access the form (using a menu or any application that calls that form, including Row and Form exits) EnterpriseOne prevents them from accessing that form.

Security can be controlled from users and groups using the following features:

- Action Security
- Table Column Security
- Table Row Security
- Processing Option Security

For all security, you can identify which application, form, report, or table you want to secure. Example: Use the object name, such as F03012 for the Customer Master file, P03013 for the Customer Master application, or *ALL for all objects.

For only row and column security, identify which columns (data items) you want secured. This is the data dictionary item name, such as ACL for the Credit Limit field, or TRA0 for the Payment Term. Column security can apply to dictionary items that are not in database tables.

To accurately determine who can add, change, or delete data in an application, form, report, or table we must look at the combination of security type, user ID, object name, data item, and from/through data value.

We must also identify all tables and then determine which applications can update the table. This must be done for each table in JD Edwards EnterpriseOne.

Copyright© 2005 Klee Associates, Inc.

JDEtips Knowledge Express

This Article Continues…

Subscribers, log in from our main search page to access the full article:

www.JDEtips.com/MyAccess.html

Not a Subscriber? Gain access to our full library of JDE topics:

www.JDEtips.com/JD-Edwards-Library

Visit **www.JDEtips.com** for information on the JDEtips University schedule, private training and consulting, and our Knowledge Express Document Library.

License Information: The use of JDE is granted to JDEtips, Inc. by permission from J.D. Edwards World Source Company. The information on this website and in our publications is the copyrighted work of JDEtips, Inc. and is owned by JDEtips, Inc.

NO WARRANTY: This documentation is delivered as is, and JDEtips, Inc. makes no warranty as to its accuracy or use. Any use of this documentation is at the risk of the user. Although we make every good faith effort to ensure accuracy, this document may include technical or other inaccuracies or typographical errors. JDEtips, Inc. reserves the right to make changes without prior notice.

Oracle and J.D. Edwards EnterpriseOne and World are trademarks or registered trademarks of Oracle Corporation. All other trademarks and product names are the property of their respective owners.

Copyright © by JDEtips, Inc.