JD Edwards EnterpriseOne

WHITE PAPER

Top 10 Security Practices You Should Know Before They Cost You Your Job!

DECEMBER 2016

ORACLE Gold Partner

Q Software

Efficient, Sustainable Controls to Protect Your Business

www.qsoftware.com

For JD Edwards EnterpriseOne:

Top 10 Security Practices You Should Know Before They Cost You Your Job!

CONTENTS

US Headquarters:
4600 S Syracuse Street, 9th Floor,
Denver, CO 80237-2719
Tel: 303-256-6630

UK & EMEA Headquarters:
Connect House, Kingston Road,
Leatherhead, KT22 7LT United Kingdom
Tel: +44 (0) 1372 700852

sales@qsoftware.com

EXECUTIVE SUMMARY

Understanding JD Edwards security can be overwhelming, due to its layers of complexity and various components involved in compliance.

With an ever increasing focus on compliance, it becomes difficult to understand the top priorities for implementation to ensure you reduce the risk of fraudulent activity within your organization. No longer is it just about the security workbench and its records; now you need an all-encompassing security strategy.

We aim to deliver key practices that make up an effective security strategy for JD Edwards - practices you should know before they cost you your job. Processes, procedures, models, reviews and databases all serve as important elements of this strategy.

This paper describes ten security practices to consider implementing as part of your strategy. The practices are easy to implement and can be adopted using various tools.

The top 10 security practices covered are:

- User Profile Management
- Periodic User Access Reviews
- User Categorization
- Authentication
- Default Account Passwords
- Security Model
- Change Management
- Database Access Management
- Segregation of Duties
- Segregation of Duties Reviews

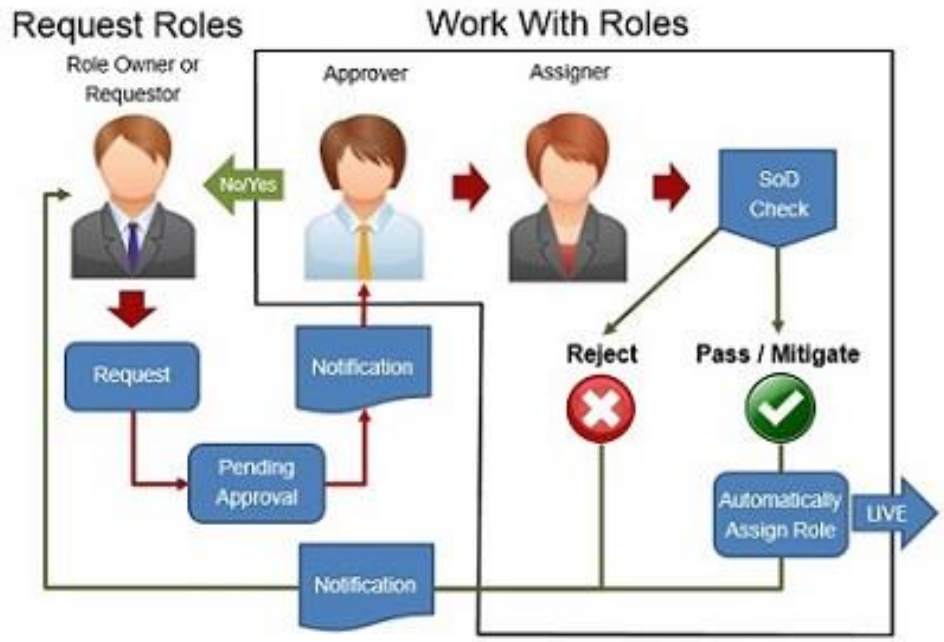
It describes in detail how implementing these top practices will significantly reduce your risk of fraud and enhance compliance within your company.

USER PROFILE MANAGEMENT

User profile management refers to the various stages a user will go through during their 'life' within the JD Edwards application. Managing users can be a long-winded and tedious task due to the fact you have to perform actions one by one in various screens. This leaves room for error in a highly audited part of your system.

Understanding and documenting the User Profile Management process is key to maintaining compliance.

It is important that distinct processes are created for managing role assignments within your company. Role requests, approvals and notifications should all be considered (terminations and users moving to other job functions should not be forgotten). Below is a high level example of the User Profile Management process where each task is identified and the requestor, approver and assigner are all separate individuals.



In addition to distinct processes, procedural documents should also be created to ensure standardization of tasks. Creation of a user ID for example, can be documented with details such as: applications utilized, checks for active address book number (noting any unauthorized search types), User ID formats, user password setup and proxy ID setup.

Finally, it is recommended proactive Segregation of Duties checking be in place to further reduce the risk of fraud. Validation should occur prior to role assignment to ensure the risk of fraud is not introduced. If mitigating circumstances exist they should be identified and noted.

PERIODIC USER ACCESS REVIEWS

Once the user management process is defined, the next step is to perform periodic user access reviews.

These reviews help ensure that necessary personnel have appropriate system access. Defining the scope of the review is critical and should involve a risk based approach that is process centric. Business owners should be identified either by JDE application or module, the data within their applications should be classified and access rules defined (what applications should and should not be accessed by users assigned to the applicable role). Documentation can then be created to identify procedures for obtaining the data and state the expectations for reviewers.

System generated user access lists are the ideal reporting mechanism for both business owners and auditors.

User access reviews typically consist of the following data:

- User ID (all types – employee, contractor, system)
- Address book number
- Job title
- Business unit or department
- Supervisor
- Role
- Application
- Privileges (read only, update, delete).

Frequency of user access reviews can be based on things such as the amount of risk associated with the access being reviewed, the amount of change observed within the environment or stability (or lack thereof) of documented procedures. It is recommended the review be performed at least on a quarterly basis.

Data for the review should be generated from the production environment and distributed to business role owners or representatives. The owners are then accountable for performing the review with a focus on:

- Ensuring the users listed should have access to the system
- The access is in accordance with defined access rules
- The access is appropriate for the users' job function
- If the access is temporary and exception based, the details have been noted along with any compensating controls
- The access was provisioned according to your User Management process.

Privileged access, also referred to as sensitive or elevated, is most often assigned to system administrators, developers or support personnel. These users are typically granted wider access to the system in order to administer, troubleshoot and provide support to others. It is recommended a review be conducted for these types of users on a more frequent basis.

USER CATEGORIZATION

Following the topic of user access reviews, it is not only important that users are categorized but also that the classification can easily be applied, as it assists you with efficient reporting. Not all users of the JD Edwards application are defined as end users. Often there are generic users that are used for training, testing and services. Having a categorization strategy that is included in the user management process can dramatically increase compliance.

The most popular categorizations used for JDE users are by:

- Module
- Access
- Provider
- Usage

Module	FIN	Finance
	SCM	Supply Chain Management
	JC	Job Cost
Access	INQ	Inquiry
	UP	Update Only (add, change)
	FULL	Add, Change, Delete
	DL	Delete Only
Provider	E	Employee
	C	Contractor
Usage	SCH	Scheduling
	TST	Testing
	TRA	Training

Categorization of user IDs is often overlooked and can be easily applied based on JDE release and security tool. Here are three solutions to investigate:

1. Business preferences located under the form exit within the User Profile Revisions application (P0092)
2. Category Codes located in the Cat Code tabs of the Address Book Revisions application (P01012)
3. Q Software Reporting codes located in various software products such as Profile Manager, Security Manager Pro and Audit Manager.

Once users are categorized, you can configure your reports and enhance your compliance, especially around those often forgotten but highly audited service IDs.

AUTHENTICATION

It is crucial that user authentication is required to access your JD Edwards application. Passwords standards must be defined as part of a corporate policy and follow industry best practices. The policy can then be configured within the EnterpriseOne Security application.

Documented within your password policy should be items such as:

- Minimum length
- Expiration
- Invalid attempts until lockout
- Password history
- Following a new user's initial sign on to the program, the user is prompted to change the password
- Passwords are encrypted or masked

It is recommended a two part review be conducted either quarterly or annually to not only ensure JD Edwards continues to adhere to your corporate password policy but also that the policy is actually being applied to users.

Part one of the review can simply consist of screen shots of the processing options for the Enterprise One security application (P98OWSEC) and part two is a system generated listing of each user, showing password settings with the goal of identifying exceptions.

Key columns in the review include:

User ID	Change Frequency	Last Change	System User	Force Immediate Password Change	Daily Password Change Limit	Password Change Counter	Allowed Attempts	Enabled User	Retry Count

Exceptions to the password policy should be reviewed and approved by management. Exceptions often related to User IDs are those used for third party scheduling tools or integrations with timed connectivity such as BSSV.

DEFAULT ACCOUNT PASSWORDS

JD Edwards is shipped with a set of standard system / service user IDs, the most recognized of these IDs being the "JDE" ID itself. Passwords for these IDs are predefined by Oracle and are widely known and easily obtained. The IDs exist for the front end application and the database. These default passwords must be changed to reduce the risk of fraud within your JD Edwards system.

JD Edwards user IDs out of box are IDs such as:

- APPLEAD
- JDEDBA
- DV900
- PS900
- SVM900
- PRODCTL
- JDE

Changing the passwords immediately after installation is best practice, followed by a documented process for quarterly or annual change. Users, especially those with elevated access such as system administrators, come and go so it is imperative to have this operational change in place.

The process should contain key tasks such as:

- Review and approval of the user IDs where the passwords will be changed on a periodic basis by management
- Calendar dates set forth on when the change will occur
- Procedural documents indicating the steps for change
- Extract of the data to confirm the change was completed as per schedule.

Passwords are typically changed during an outage window with the new password being stored in a secure area, where specific users such as system administrators are granted specific access to view the file.

JD EDWARDS SECURITY MODELS

JD Edwards security is typically implemented using one of two security models known as 'All Doors Open' or 'All Doors Closed'.

All Doors Open (ADO)

Out of box JD Edwards is delivered with an All Doors Open security model, which is where access is granted to all objects. Users have the ability to run all applications, reports and have access to all data. Access must then be denied for items the user should not have access to and is typically done either by menu filtering or entering specific security records in the security workbench. The open model is often chosen as it is easier for users to specify what they shouldn't have access to then specify all the items they do need access to. It is perceived as quick setup and causes the most issues from a compliance and audit standpoint.

Example of ADO in the Security Workbench:

User / Role	Object Name	Security Type	Description	Add	Change	Delete	OK/Select	Copy	Scroll to End	Run	Install
*PUBLIC	*ALL	1	Action Security	Y	Y	Y	Y	N	Y		
*PUBLIC	*ALL	3	Application Security							Y	Y

Go ADC!
All Doors Closed is the most compliant and recommended security model.

All Doors Closed (ADC)

To protect systems from unauthorized access, leading auditors advise companies to implement an All Doors Closed model. Access is denied and only those applications, reports and data the user requires access to are granted back. This approach assures there are no missed objects and dramatically reduces the risk of unauthorized access. The closed model can take longer to implement as there are many associated objects, reports and hidden programs to consider, however third party security tools can drastically decrease the time required.

Example of ADC in the Security Workbench:

User / Role	Object Name	Security Type	Description	Add	Change	Delete	OK/Select	Copy	Scroll to End	Run	Install
*PUBLIC	*ALL	1	Action Security	N	N	N	Y	N	N		
*PUBLIC	*ALL	3	Application Security							N	N

To determine what security model is implemented in your JD Edwards system simply follow the steps below:

1. Access the Security Workbench Application (P00950)
2. In the User / Role column enter '*PUBLIC'
3. In the Object Name column enter '*ALL'
4. Review Application (3) and Action (1) security types.

CHANGE MANAGEMENT PROCESSES AND REPORTING

To implement change within your JD Edwards system you should implement a change management process. The process must be controlled, monitored and cover both standard and emergency changes.

Key activities within the standard process include:

- Request for change is documented
- Solution is created by developers and deployed to the development environment, where it is unit tested
- Once solution passes unit testing, it is deployed to the prototype environment, where further testing occurs by a functional or business representative
- Once the solution passes functional testing it is deployed to the quality assurance environment, which is a replication of production and tested by business representatives
- Should the solution pass testing it is then approved by a management authority such as supervisor or leader for the move to production
- Once approved the solution is then deployed to production by a system administrator.

Access to the Object Management Workbench should be restricted to those where it is appropriate for their job function. Separate roles should be created for developers, testers, approvers, system administrators and change management personnel.

Periodic reviews should take place and include items such as:

- User access
- Projects are tested throughout the various environments prior to being deployed to production
- Projects deployed to production have corresponding management level approval prior to the deployment.

JD Edwards out of box provides a number of reports related to change management such as:

- R98210A – Object Management Log Report
- R98221A – Project Users Report
- R98223A – User Allowed Actions Report.

DATABASE ACCESS MANAGEMENT

Access to the JD Edwards database is often an afterthought for most companies. Just as it is important to secure the front end application, security to the database should also be considered.

Similar to the application, you can create roles and grant permissions on the database, such as read only or read / write. Database administrators, system administrators, developers and even support personnel require access and therefore it should be carefully planned and organized.

It's not enough to secure the front end application;
FRAUD KNOWS NO LIMITS!

Below is an example of report specifics for consideration:

Username	Job Title	Business Unit	Supervisor Name	DB Access	Account Status	Access Type	Actions	Schema	Account Type
				JDE_CONNECT	OPEN	ROLE		PRODCTL	DBA
				JDE_SELECT	LOCKED	TABLE	READ		SUPPORT
				JDE_UPDATE	LOCKED (TIMED)		UPDATE		DEVELOPER
				JDE_HR_SELECT					
				JDE_HR_UPDATE					

A standard password policy can be placed within a specific role such as JDE_CONNECT. For IDs that do not adhere to the standard, a separate connect role with those differing standards can be created. This is also an effective method of identifying generic versus end users.

In addition to the above, the following points will also ensure compliance:

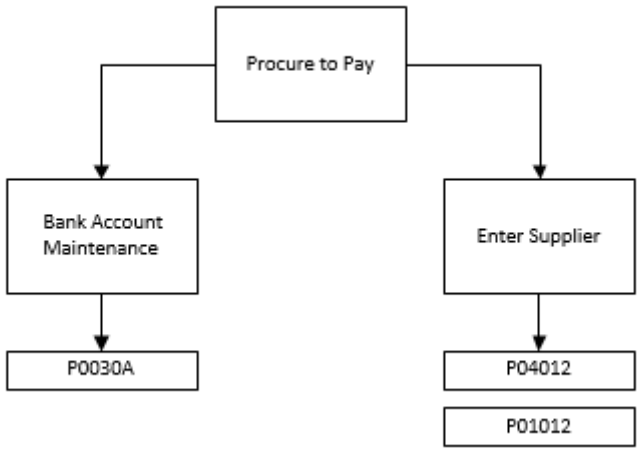
- User Profile Management processes and procedures should exist for database access
- User categorization can be achieved through naming conventions for those generic and service type accounts, to differentiate them from other user types
- User ID and passwords are required to access the database
- Minimize group / shared ID access to the database
- Database password controls are consistent with those contained in your corporate password policy
- Change Management process exists and is followed for all database changes
- Backup and recovery procedures are not only in place but tested on a recommended annual basis
- It is recommended reviews take place on a quarterly basis.

SEGREGATION OF DUTIES RULES

Whether you are a publicity traded company that must adhere to regulatory requirements like Sarbanes-Oxley legislation or a private company following best practice, you should have the ability to enforce effective Segregation of Duties controls. Segregation of Duties (SoD) is the concept of requiring more than one person to complete a task. No one person should have access that allows them to execute two or more transactions that have the potential to impact financial statements.

SOX regulations can and should be applied to all companies. Fraud is just as likely to occur in private companies as public

Below is an example of a Segregation of Duties rule within the Procure to Pay process. A single person should not have access which allows him/her to enter a supplier and add bank account details for that supplier. This could allow a user to enter a fictitious bank account or modify an existing bank account and assign it to a supplier of their choice.



In determining SoD rules consider the following steps:

1. Select a business process
2. Identify key responsibilities within the business process
3. Of those responsibilities, identify any regulatory requirements, conflicts or business reasons where fraudulent activity may occur, resulting in impacts to financial statements
4. Identify any unique application customizations
5. Identify any risk mitigation methods currently in place.

SEGREGATION OF DUTIES REPORTING

Segregation of Duties checks should occur:

1. Prior to assignment of roles to a user ID
2. Prior to a security change
3. As a regular overall check.

Using your established Segregation of Duties rules you must then start to proactively check for violations to SoD rules. As this is a complex exercise we recommend utilizing a third party security tool.

Segregation of Duties reporting involves:

- Creation of rules within the tool (application and action level)
- Execute reporting within the tool
- Analyse output
- Enter mitigations.

Violations can occur within roles themselves, by users with access to multiple roles or by users with access to multiple roles across different applications. To resolve violations you must choose to make a security change within a role, remove a role from a user or enter a mitigation.

Entering a mitigation, such as those for system administrators with full access, should require a compensating control to be in place. Typically a form of database monitoring is utilized to track transactions such as adding new users, changing UDC values or creating an invoice.

Q Software

An Independent Software Vendor and Oracle Gold Partner, Q Software delivers security and compliance solutions and services for users of JD Edwards EnterpriseOne, JD Edwards World, and Oracle E-Business Suite. Our products help customers to protect their businesses from fraud whilst significantly reducing the cost, effort and complexity of managing risk and demonstrating regulatory compliance.

If you would like to discuss any of the points raised or find out more about how our products and services can help you, please email your Q Software contact or sales@qsoftware.com or visit www.qsoftware.com