Technical / Security

Compliance Reporting on JDE E1 Security

What is Available and Where to Start

By Alex Rippingale, ALLOut Security

Editor's Note: Most organizations realize the importance of securing their data and access to that data. They go to great lengths to ensure that security is set up properly, in accordance to their own specific business requirements. In addition, regulations such as Sarbanes-Oxley in the US have increased the need for, awareness of, and thoroughness of security reporting requirements. However, security setup in JDE E1 is the key, and can be an onerous and complex task. In this article, Alex Rippingale from ALLOut Security breaks down the issue of compliance reporting into four key areas and explains how to best address the setup for each area. These concepts of User Security Access, Data Access, Segregation of Duties, and Access Auditing are discussed in a way that's much easier to understand.

Introduction

This article will discuss the complex subject of compliance in a JD Edwards (JDE) EnterpriseOne (E1) system. In order to determine compliance, reports must be produced showing what authority users have to process or update sensitive data pertinent to each individual business. Subsequently, these reports can be approved and additional controls applied if required.

How to effectively prove compliance in a JDE E1 environment covers a range of topics, each of which is broken down within this document:

User Security Access	There are several security related factors that control how users' access and employ programs in JDE E1. All these factors must be considered when working out what access users have within the system.
Data Access	Access to data is impacted via programs, but the data itself can also be protected using data security features inherent in JDE E1 (e.g. Row Security). Typically, this takes the form of only allowing access to the Companies and/or Business Units that individuals require. Proving this data access forms part of compliance reporting.
Segregation of Duties	In order to demonstrate compliance, it is not enough to just show who has access to individual programs; it must also be proven what processes individuals can perform. Each process must be investigated and access to multiple processes established to ensure that any risk of fraud is highlighted. Effective controls should also be put in place to ensure that the associated risk is mitigated.
Access Auditing	Establishing what access users have to the programs is one step in reporting on access compliance. It is also important to show what security changes were made, when the changes occurred, and who was responsible for any changes. This can also be useful from a troubleshooting perspective.

User Security Access

EnterpriseOne (E1) uses the security records within its F00950 table to control authorities on the system. To control access (and therefore become compliant) this typically consists of two main security types at the program level:

Application security (type 3)	This includes a permission flag that determines whether end users can or cannot run a program (i.e. Run set to Yes or No).
Action Code security (type 1)	This includes permission flags for actions that interactive applications use to update data (i.e. Add/Change/Delete/Copy set to Yes or No). This typically translates as whether a program is view only or update capable for an end user.

Security Hierarchy

Security in E1 can be applied to users, the users' assigned roles (known as the *Group in older versions of E1), and to a *PUBLIC role that is automatically assigned to all users – within the E1 application (i.e. not against the database profile or other external applications).

The Security Hierarchy is the order in which security records are read by the system to determine what authority a user has. This translates as a user's 'Effective' access.

The records are always read in User, Role, and then Public sequence as shown in Figure 1.