ALLOut Security

Security Audits

ALLOut Audit Assessments & Verifications Catalog

Version 2

Updated November 2024

ALLOut Audit Assessments & Verifications Catalog

Enforcing GRC controls and managing risk in JDE — including:

- Segregation of Duties enforcement and breach mitigation
- User provisioning and privileged user access
- Ongoing User Access Reviews and data security
- Control testing and transaction monitoring
- Audit preparation and risk-focus analytics

ALLOut Audit Assessments & Verifications Catalog

Your choice of audits

- ✓ JD Edwards Security & Compliance Assessments
- ✓ JD Edwards Access Controls (in ALLOut Product) Verifications

FAQs:

What is an ALLOut Audit?

An ALLOut Audit is a brief (typically one-day) engagement with a standard agenda. It provides Customers with a written deliverable to support decision-making.

How can an ALLOut Audit help us?

- ✓ A **JD Edwards security & compliance assessment** evaluates your current risk exposure within JD Edwards, based on your existing security setup. It is designed to help you identify the next steps to improve security and compliance at your own pace, whether that means planning a project, hiring additional resources, or utilizing more ALLOut product functionality.
- ✓ An **ALLOut product verification** reviews your current ALLOut implementation to confirm that your JD Edwards access control and auditing capabilities meet your requirements.

Are the audits (either assessments or verifications) interactive?

No, these audits do not involve full-service, fact-finding discussions.
Once we have access to your system, no additional customer time is required.
We will email you a comprehensive report of our findings within days of completing the agenda.

Is the report certified by an independent body?

We are an Oracle-certified partner and the only organization focused exclusively on JD Edwards security. Our reports can help demonstrate effective progress to management and auditors.

Who can request an audit?

Any JD Edwards customer can request an audit, and some assessments do not require ALLOut software.

How can we schedule an audit?

If you believe an audit could benefit you, log in to our Customer Portal and contact the Customer Success team. We use a brief "Statement of Work" document to establish agreement on the defined agenda. Once signed, sessions can be scheduled.

Can ALLOut provide IT services beyond those listed on the website?

No, our focus is software development, and our aim is to guide you in taking ownership of your system.
For ALLOut product training, consider our Consulting Academy or training workshops available in the Customer Portal.
If you need hourly or similar services, we can recommend providers from our extensive partner network of specialized service providers.

All audits come with a predefined agenda and length

JD Edwards Security & Compliance Assessments

1. Security Assessments – without installing ALLOut software (ASSESS1)

A – High-Level Security Review (2 x 3-hour sessions)

The audit deliverable is an ALLOut-certified assessment of the current access permitted to your JD Edwards system and the risk exposure resulting from that access.

The objective is to identify if there are critical areas of risk, give a high-level opinion on potential Segregation of Duties exposure, and make workable suggestions to guide effective mitigation.

The engagement requires access to JD Edwards Data Browser only – no ALLOut software is used.

B – Comprehensive (on exported data) SoD & System Access Assessment (4 x 3-hour sessions)

The audit deliverable is a comprehensive ALLOut-certified assessment of the current access permitted to your JD Edwards system and the risk exposure resulting from that access.

The objective is to identify critical areas of risk and guide effective mitigation efforts with particular attention to Segregation of Duties exposure.

The engagement requires a copy of your security data to be exported – no ALLOut software is installed on your system.

2. Security Assessments – using installed ALLOut software (ASSESS2)

A – InfoSec Security Assessment (for ISO/IEC) (3 x 3-hour sessions)

The audit deliverable is an ALLOut-certified assessment of the effectiveness of your current JD Edwards security and system access controls including change management and monitoring.

The objective is to assess the completeness of existing policies and identify any potential improvements. The audit is intended to prepare the ground for Segregation of Duties initiatives, support internal compliance and ensure readiness for external audits.

B – Segregation of Duties Risk Analysis (2 x 3-hour sessions)

The audit deliverable is an ALLOut-certified assessment of your current Segregation of Duties exposure within your JD Edwards system based on a full SoD report and relevant analysis of underlying security.

The objective is to identify critical areas of risk and guide effective mitigation efforts with suggestions of current remediation and mitigation strategies available.

C – User Access Review: Functional (Program) Access (2 x 3-hour sessions)

The audit deliverable is an ALLOut-certified assessment of the current User (and role) access permitted to your JD Edwards system and any risk exposure resulting from that access.

The objective is to identify critical areas of risk and guide effective mitigation efforts of any excessive functional access.

D – User Access Review: Company (Data) Access (2 x 3-hour sessions)

The audit deliverable is an ALLOut-certified assessment of the current User (and role) access permitted to your JD Edwards system in a multi-company environment where access to each company's data needs to be controlled independently.

The objective is to identify critical areas of non-compliance and guide effective mitigation efforts of any unauthorized access.

3. Compliance Assessments – using installed ALLOut software (ASSESS3)

A – JDE Personal Data Regulatory Risk (GDPR/CCPA) (2 x 3-hour sessions)

The audit deliverable is an ALLOut-certified assessment of the personal data that is currently stored within your JD Edwards system and current measures to limit access to that data.

The objective is to identify the personal data that should be removed or be subject to restricted access if retained.

B - Oracle User Licensing for JD Edwards (2 x 3-hour sessions)

The audit deliverable is an ALLOut-certified assessment of the number of users that are currently actively using the different modules of your JD Edwards system.

The objective is to provide the information necessary to enable accurate licensing of JD Edwards products including guiding the removal of any inactive User profiles.

JD Edwards Access Changes & Controls Verifications

4. ALLOut Product Verifications – of installed ALLOut software (VERIFY1)

A – JDE Access (Changes) Auditing Verification (1 x 3-hour session)

The audit deliverable is an ALLOut-certified verification of the auditing data capture of your JD Edwards system access and change controls, and the extent to which your audit processes can be effective.

The objective is to provide management with concise information and to identify any potential improvements to current auditing activities.

B – JDE Access (Changes) Controls Verification (1 x 3-hour session)

The audit deliverable is an ALLOut-certified verification of your current system access (security and role) change control processes, and the extent to which your change control processes can be effective.

The objective is to provide management with concise information and to identify any additional controls that could prevent unwanted system access.

C – ALLOut Post-Upgrade/Install Functionality Verification (2 x 3-hour sessions)

The audit deliverable is an ALLOut-certified verification of previously implemented ALLOut features – typically following an implementation or software upgrade.

The objective is to provide management with concise information and to identify any features that could be easily adopted by your business to provide value without additional investment.