ALLOut Security

Security Audits

ALLOut Audit Assessments & Verifications Catalog

Version 2

Updated October 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

JD Edwards Security & Compliance Assessments

JD Edwards Access Controls Verifications

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 a JD Edwards Security & Compliance assessment?
It is a focused assessment of your current risk exposure within JD Edwards as determined by your current security. Depending on your concerns and previous efforts at mitigation, choose the assessment that is closest to your needs.

What is an ALLOut product verification?
It is a verification that your current ALLOut implementation provides you with the JD Edwards access control and auditing capability that you need.

Are the audits (either the assessments or the verifications) interactive?
No, they are intentionally auditing only with a standard agenda for delivery in 3-hour sessions.
If you are looking for training, consider our training workshops as advertised within the Customer Portal.

How do we receive the results of the audit?
We will deliver a report of our findings to you so that you can take the next appropriate steps.

Is the report certified by an independent body?
We are an Oracle-certified partner, and the only organization that uniquely focuses on JD Edwards security. Our reports can help you show effective, demonstrable progress to management and auditors.

Who can request an audit?
Audits are available to any JD Edwards user. Some assessments do not require the installation of ALLOut software.

Does there need to be a signed agreement?
Yes, we use a very brief 'Statement of Work' document to ensure agreement to follow the clearly defined agenda.

How can we schedule an audit?
If you believe an audit can help you, log on to our Customer Portal and contact the Customer Success team.
Once the agreement is signed, session(s) can be scheduled.

Can ALLOut provide IT services in addition to those advertised on the website?
No, our business is software development - our aim is to guide you in taking ownership of your system.
If you require 'hourly-rate' or similar services, we recommend from amongst our extensive partner network of specialist service-providers.

All audits come with a predefined agenda and length

JD Edwards Security & Compliance Assessments

1. Security Assessments – without installing ALLOut software (AUD1)

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 (AUD2)

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 (AUD3)

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 Controls Verifications

4. ALLOut Product Verifications – of installed ALLOut software (AUD4)

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

The audit deliverable is an ALLOut-certified verification of your current access audit and review processes, and the extent to which security changes may be effectively audited.

The objective is to verify the effectiveness of current access audit or review processes and identify any potential improvements.

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.

The objective is to verify the effectiveness of current ALLOut change controls and identify any potential improvements. The audit is intended to support internal compliance and ensure readiness for external audits.

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

The audit deliverable is an ALLOut-certified verification of your ALLOut implementation – typically following an implementation or upgrade.

The objective is to verify the effectiveness of previously implemented features and highlight any features that could provide additional value specific to the Customer's current circumstances. The audit is intended to support internal compliance and decision-making,