ALLOut Security

Security Audits

ALLOut Catalog of JD Edwards Security Audits

from the only Oracle-certified partner focused exclusively on enforcing security controls and managing GRC risk in JD Edwards

Version 2.2

Updated April 2026

ALLOut Catalog of JD Edwards Security Audits

Your choice of 1-day* audit:

(* based on 2 audit credits. see next pages for details)

1) To support internal decision-making, prior to using ALLOut, choose:
   - **JD Edwards Security Assessment (ASSESS)**
     - Indicative view of security effectiveness
     - Assessment of potential excessive access and Segregation of Duties exposure
2) To prepare for an external audit (after ALLOut implemented), choose:
   - **JD Edwards Access Review (REVIEW)**
     - Documented evidence of security effectiveness
     - Identification of actual excessive access risk and Segregation of Duties exposure
3) To prepare for regulatory or compliance checks (with ALLOut installed), choose:
   - **JD Edwards Compliance Review (COMPLY)**
     - Documented evidence of compliance position
     - Assessment of regulatory (GDPR/CCPA) and licensing (Oracle) exposure
4) To confirm risk is detected and prevented (after ALLOut implemented), choose:
   - **ALLOut Control Verifications (VERIFY)**
     - Documented evidence of ALLOut control effectiveness
     - Validation of effective ALLOut product usage, detecting and preventing risk

FAQs:

What is an ALLOut Audit?

An ALLOut Audit is a brief (typically one-day) engagement which follows any of the preset agendas listed in this document. The purpose is to provide Customers with a comprehensive written deliverable to support internal decision-making and/or to provide documentary evidence to support internal compliance with external audits.

Can the audits be interactive?

No, these audits are not consulting - once we have access to your system (or to your security data), your time is not required. We will email you a comprehensive report of the findings within days of completing the agenda.

Who can request an audit?

Any JD Edwards customer can request an audit (our audit reviews do not require ALLOut software). If you believe an audit could benefit you, contact our Sales team or log onto your Customer Portal and contact Customer Success. We use a brief "Statement of Work" contract to confirm your chosen agenda.

Can ALLOut provide IT consulting services?

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

1. ASSESS: JD Edwards Security Assessments

Supporting internal decision-making – without ALLOut software

These engagements do not require installing ALLOut software – just a copy of your exported JD Edwards security data, or alternatively, view-only access to your JD Edwards system.

For a comprehensive audit using ALLOut-for-E1 software, request a REVIEW audit below.

Agenda A (5 Audit Credits): **Security Policies & Access Assessment** of your exported security data

Deliverable: An ALLOut-certified report providing a comprehensive assessment of your current JD Edwards security policies and access control framework, together with a high-level assessment of the current access permitted within your JD Edwards system, and the risk exposure, evidenced by excessive access and Segregation of Duties breaches.

Approach: The audit is conducted by analyzing **your exported JD Edwards security data** using our purpose-built **Audit Analysis AI Tool.**

Agenda B (2 Audit Credits): **Security Policies Only Assessment** using Databrowser in your system

Deliverable: An ALLOut-certified report providing an indicative assessment of your current JD Edwards security policies and access control framework, and the likely risk exposure resulting from those policies (excessive access and Segregation of Duties breaches).

Approach: The audit is conducted using **Data Browser in your JD Edwards** only.

Your data will not be copied or exported. No changes will be made within your system.

2. REVIEW: JD Edwards Access Reviews

Preparing for external audit – using ALLOut software

These engagements require access to your system using Teams or Quick Assist.

ALLOut software must be pre-installed and the product license active. Version 4.1 is advised.

Audits are conducted using ALLOut reports and inquiries, and JD Edwards Data Browser only.

Your data will not be copied or exported. No changes will be made within your system.

Agenda A (2 Audit Credits): **Security Policies & Controls Review** for InfoSec & ISO/IEC standards

Deliverable: An ALLOut-certified report providing a review of the effectiveness of your current JD Edwards security and system access policies, including controls and monitoring, designed to assess the effectiveness of the existing approach and identify areas where controls may be insufficient.

Agenda B (2 Audit Credits): **Segregation of Duties Risk Review:** Breaches & Mitigating Controls

Deliverable: An ALLOut-certified report providing a review of your current Segregation of Duties exposure within your JD Edwards system, using identified rules and any documented mitigations, with relevant analysis of underlying security, designed to highlight critical risk areas of risk and potential control gaps.

Agenda C (2 Audit Credits): **User Access Review** of Functional and Data Access

Deliverable: An ALLOut-certified report providing a review of the User (and role) access that is currently permitted within your JD Edwards system and any risk exposure resulting from that access.

3. COMPLY: JD Edwards Compliance Reviews

Supporting regulatory and external compliance – using ALLOut software

These engagements require access to your system using Teams or Quick Assist.
ALLOut software must be pre-installed and the product license active. Version 4.1 is advised.
Audits are conducted using ALLOut reports and inquiries, and JD Edwards Data Browser only.
Your data will not be copied or exported. No changes will be made within your system.

Agenda A (3 Audit Credits)**: Personal Data in JD Edwards:** Regulatory Risk with GDPR, CCPA etc.

Deliverable: An ALLOut-certified report providing a review of the personal data currently stored within your JD Edwards system that should be removed or otherwise subject to restricted access, and the current measures in place to limit access to that data.

Agenda B (3 Audit Credits): **Oracle User Licensing** for JD Edwards

Deliverable: An ALLOut-certified report providing a review of active user counts for all your JD Edwards modules, with the information necessary to enable accurate licensing of JD Edwards products, and the impact of removing unnecessary user profiles.

4. VERIFY: ALLOut Control Verifications

Validating ALLOut software configuration to detect & prevent risk in JD Edwards

These engagements require access to your system using Teams or Quick Assist.
ALLOut software must be pre-installed and the product license active. Version 4.1 is advised.
Audits are conducted using ALLOut reports and inquiries, and JD Edwards Data Browser only.
Your data will not be copied or exported. No changes will be made within your system.

Agenda A (2 Audit Credits): **ALLOut Product Usage** of Installed Software

Deliverable: An ALLOut-certified verification of current ALLOut product usage, including implemented and available features – typically following product implementation or software upgrade – to assess the security policies and controls managing access within your JD Edwards system.

Agenda B (2 Audit Credits)**: Security Change Management:** Risk Prevention in JD Edwards

Deliverable: An ALLOut-certified verification of your security change controls, assessing whether they provide effective control over ongoing changes to security access within JD Edwards.

Agenda C (2 Audit Credits)**: Access Change Auditing:** Risk Detection in JD Edwards

Deliverable: An ALLOut-certified verification of your post-change (detective) audit review processes, assessing whether they provide effective oversight of ongoing changes to security access within JD Edwards.