Assess Risk Exposure -> Review & Comply -> Verify Risk Controls

JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

ASSESS – JDE Security Assessments
(**without** installing ALLOut software):

A –Security Policies & Access Assessment
(using our Audit Analysis AI Tool on exported copy of your security data)

B –Security Policies Only Assessment
(using JDE Data Browser on your system)

REVIEW - JDE Access Reviews
(**using** your installed ALLOut software):

A – Security Policies & Controls Review
(for InfoSec & ISO/IEC Standards)

B – Segregation of Duties Risk Review
(Breaches & Mitigating Controls)

C – User Access Review
(of Functional and Data Access)

COMPLY – JDE Compliance Reviews:
(**using** your installed ALLOut software):

A – Personal Data in JD Edwards
(Regulatory Risk with GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – ALLOut Control Verifications:
(validating **your** installed ALLOut software):

A –ALLOut Product Usage
(Making the Most of ALLOut)

B – Security Change Mgmt. in JD Edwards
(Preventing Unauthorized Access.)

C – Access Change Auditing in JD Edwards
(Detecting Unauthorized Access.)

JD Edwards Compliance Reviews (COMPLY-A)

Personal Data in JD Edwards:
Regulatory Risk with GDPR, CCPA etc.
(using your installed ALLOut software)

Synopsis:

Assess the risk exposure to personal data within your JD Edwards system

"Get clarity from the specialist JD Edwards security company"

Personal Data in JD Edwards: Regulatory Risk with GDPR, CCPA etc.

(using your installed ALLOut software)

Key Features

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.

Approach: The audit is conducted using **ALLOut reports and inquiries** (via menu program PAOS0001), and the JD Edwards Data Browser only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Provide documentary evidence to support internal compliance.

Engagement

Three Audit Credits – allocated to:

- One 3-hour session - **with 'take control' access to your system using Teams or Quick Assist**
  - If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - ALLOut software must be pre-installed and the product license active.
  - ALLOut for E1 Version 4.1 is advised.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Identify Personal Data within JD Edwards:

- HR data (e.g., F060116).
- Address book (e.g., F0111).
- Media object attachments (i.e., F00165).

Assess Exposure of Personal Data:

- Verify use of Data Masking security (F00950):
  - Media Object security – for images and contracts.
  - Address Book Data Privacy – for telephone numbers, email, and physical addresses.
  - Row Security – for sensitive data in relevant tables (e.g., within HR module).
  - Column security.
- Assess (IT) account access vulnerability:
  - Developer Access to production is not available (enabled by separate roles with F0093).
  - JD Edwards accounts are separate from database accounts (F98OWPU).
  - Access to OMW (P98220) is limited (F00950).
  - Non-prod environment access limited to privileged accounts (F0093).
  - Personal data removed from sandpit and developer systems (F0101).
- Assess Business User System Access:
  - Role-based deny-all and grant-back access (F00950).
  - Limiting Read-only access with FastPath security (F00950).
  - Limited access to data browser (F00950).
  - Best-practice password policy (Configuration).

Assess Risk and highlight Exposure

JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

ASSESS – JDE Security Assessments
(**without** installing ALLOut software):

A –Security Policies & Access Assessment
(using our Audit Analysis AI Tool on exported copy of your security data)

B –Security Policies Only Assessment
(using JDE Data Browser on your system)

REVIEW - JDE Access Reviews
(**using** your installed ALLOut software):

A – Security Policies & Controls Review
(for InfoSec & ISO/IEC Standards)

B – Segregation of Duties Risk Review
(Breaches & Mitigating Controls)

C – User Access Review
(of Functional and Data Access)

COMPLY – JDE Compliance Reviews:
(**using** your installed ALLOut software):

A – Personal Data in JD Edwards
(Regulatory Risk with GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – ALLOut Control Verifications:
(validating **your** installed ALLOut software):

A –ALLOut Product Usage
(for Making the Most of ALLOut)

B – Security Change Mgmt. in JD Edwards
(Preventing Unauthorized Access.)

C – Access Change Auditing in JD Edwards
(Detecting Unauthorized Access.)

JD Edwards Compliance Reviews (COMPLY-B)

Oracle User Licensing
for JD Edwards
(using your installed ALLOut software)

Synopsis:

Assess your Oracle user licensing requirements for JD Edwards

"Get clarity from the specialist JDE security company"

Oracle User Licensing for JD Edwards

(using your installed ALLOut software)

Key Features

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.

Approach: The audit is conducted using **ALLOut reports and inquiries** (via menu program PAOS0001), and the JD Edwards Data Browser only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Provide documentary evidence to support internal compliance.

Engagement

Three Audit Credits – allocated to:

- One 3-hour session - **with 'take control' access to your system using Teams or Quick Assist**
  - If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - ALLOut software must be pre-installed and the product license active.
  - ALLOut for E1 Version 4.1 is advised.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Identify Potential Usage:

- Get full list of User profiles within system (PCML0960):
  - Verify if inactive Users are still enabled to access system (PDIS0300).
- Document alternative licensing methodologies:
  - Actual (past) program access (including read-only) – using 9.2 Object tracking.
  - Actual (past) program access (where data updated) – using Usage Inquiry.
  - Potential program access – using SoDMaster critical list 'LISTAUDIT' and security.

Identify Actual Usage:

- Review potential program access:
  - Time period for past access will be 6 (six) months.
- Review actual program access:
  - Module identification will be by JDE product code in UDC 98 SY.

Assess Risk and highlight Exposure

- Identify all inactive and non-production users (PDIS0300).