JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

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

A – High-Level Security Assessment
(using your JDE system without ALLOut)

B – High-Level Security Assessment
(of exported copy of your security data)

C – SoD & User Access Assessment
(of exported copy of your security data)

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

A – JD Edwards Security Essentials
(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 JDE
(Regulatory Risk for GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – JDE Access Control Verifications:
(**of your** installed ALLOut software):

A – JD Edwards Security Change Controls

B – ALLOut Functionality Effectiveness
(Post-Install/Upgrade)

JD Edwards Compliance Review (COMPLY-A)

Personal Data in JD Edwards: Regulatory Risk (for GDPR, CCPA etc.)

(using installed ALLOut software on your JDE System)

Synopsis:

A 6-hour engagement to assess the risk exposure to personal data within your JD Edwards system, and identify practical remediation – an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

Personal Data in JD Edwards: Regulatory Risk (for GDPR, CCPA etc.)

(using installed ALLOut software on your JDE System)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified assessment of the personal data that is currently stored within your JD Edwards system and current measures in place to limit access to that data. No changes will be made to your system – this engagement is to conduct an audit.

The scope is to identify the personal data that should be removed or otherwise subject to restricted access. The objective is to provide documentary evidence to support internal compliance.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session - with access to **your JDE system using Microsoft Teams** screen-sharing.
- One 3-hour session - to analyze **collected information** (further system access is not required).

Key Considerations

- If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
- An active ALLOut product subscription is required. **Version 4.1** is advised.
  - Access to your JD Edwards is to run data browser and ALLOut reports and inquiries using the ALLOut menu program (form WAOS0001B).

Audit Checklist

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 Menu Filtering (F9006) and FastPath security (F00950)
  - Limited access to data browser (F00950)
  - Best-practice password policy (Configuration)

Assess Risk and Suggest Remediation Best Practices

JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

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

A – High-Level Security Assessment
(using your JDE system without ALLOut)

B – High-Level Security Assessment
(of exported copy of your security data)

C – SoD & User Access Assessment
(of exported copy of your security data)

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

A – JD Edwards Security Essentials
(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 JDE
(Regulatory Risk for GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – JDE Access Control Verifications:
(**of your** installed ALLOut software):

A – JD Edwards Security Change Controls

B – ALLOut Functionality Effectiveness
(Post-Install/Upgrade)

JD Edwards Compliance Review (COMPLY-B)

Oracle User Licensing for JD Edwards

(using installed ALLOut software on your JDE System)

Synopsis:

A 6-hour engagement to assess your Oracle user licensing requirements for JD Edwards – an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

Oracle User Licensing for JD Edwards

(using installed ALLOut software on your JDE System)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified assessment of active user counts for all your JD Edwards modules. No changes will be made to your system – this engagement is to conduct an audit.

The scope is to provide the information necessary to enable accurate licensing of JD Edwards products, including the impact of removing unnecessary User profiles. The objective is to provide documentary evidence to support internal compliance.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session - with access to **your JDE system using Microsoft Teams** screen-sharing.
- One 3-hour session - to analyze **collected information** (further system access is not required).

Key Considerations

- If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
- An active ALLOut product subscription is required. **Version 4.1** is advised.
  - Access to your JD Edwards is to run data browser and ALLOut reports and inquiries using the ALLOut menu program (form WAOS0001B).

Audit Checklist

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 unless Customer instructs otherwise
- Review actual program access
  - Module identification will be by JDE product code in UDC 98 SY

Suggest User Clean-up

- Identify all inactive and non-production users (PDIS0300