JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

ASSESS1 - JDE Security Assessments (without installing software):

A – High-Level Security Assessment (requires access to Data Browser only)

B – Comprehensive Security Assessment (requires copy of Customer security data)

ASSESS2 - JDE Security Assessments (using installed ALLOut software):

A – InfoSec Security Assessment (ISO/IEC)

B – Segregation of Duties Risk Analysis

C – Functional (Program) Access

D – Company or Business Unit Access

ASSESS3 – JDE Compliance Assessments:

A – JDE Personal Data Regulatory Risk (GDPR/CCPA)

B – Oracle User Licensing for JD Edwards

VERIFY1 – ALLOut Product Verifications:

A – JDE Access Changes Auditing (Verification of Effective JDE Auditing)

B – JDE Access Change Controls Audit (Verification of Access Change Controls)

C – ALLOut Post-Upgrade/Install Audit (Verification of ALLOut Functionality)

JD Edwards Compliance Assessment (ASSESS3A):

Personal Data Regulatory Risk
within JD Edwards (GDPR/CCPA)

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 Regulatory Risk (GDPR/CCPA)

Scope and Deliverable

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. The audit is intended to support internal compliance and ensure readiness for external audits.

Standard Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session with **access to your system** to run ALLOut reports and inquiries and read-only access to configuration screens.
- One 3-hour session to analyze **submitted reports** (if reports are emailed to us, no further system access is required) to prepare the assessment.

Key Considerations

- The assessment assumes a subscription to ALLOut software.
- Access to JD Edwards can be through **screen-sharing** with the ability to run data browser and required reports & inquiries using the ALLOut menu program (form WAOS0001B).
  - The customer may choose to monitor the audit activity at the customer's discretion.

Standard Checklist

Identify Personal Data in JD Edwards

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

Assess Personal Data Exposure

- Verify use of Data Masking security
  - 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
  - Access to production not available (enabled by separate roles)
  - JD Edwards accounts separate from database accounts
  - Developer (OMW) access limited to privileged accounts
  - Personal data removed from sandpit and developer systems
- **Assess** Business User System Access
  - Role-based deny-all and grant-back access
  - Limiting Read-only access with Menu Filtering & E1 Pages
  - Limited access to data browser
  - Best-practice password policy

JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

ASSESS1 - JDE Security Assessments (without installing software):

A – High-Level Security Assessment (requires access to Data Browser only)

B – Comprehensive Security Assessment (requires copy of Customer security data)

ASSESS2 - JDE Security Assessments (using installed ALLOut software):

A – InfoSec Security Assessment (ISO/IEC)

B – Segregation of Duties Risk Analysis

C – Functional (Program) Access

D – Company or Business Unit Access

ASSESS3 – JDE Compliance Assessments:

A – JDE Personal Data Regulatory Risk (GDPR/CCPA)

B – Oracle User Licensing for JD Edwards

VERIFY1 – ALLOut Product Verifications:

A – JDE Access Changes Auditing (Verification of Effective JDE Auditing)

B – JDE Access Change Controls Audit (Verification of Access Change Controls)

C – ALLOut Post-Upgrade/Install Audit (Verification of ALLOut Functionality)

JD Edwards Compliance Assessment (ASSESS3B):

Oracle User Licensing for JD Edwards

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

Scope and Deliverable

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.

Standard Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session with **access to your system** to run ALLOut reports and inquiries and read-only access to configuration screens.
- One 3-hour session to analyze **submitted reports** (if reports are emailed to us, no further system access is required) to prepare the assessment.

Key Considerations

- The assessment as per the checklist below assumes a subscription to Risk Reporting (for PCML0600) with SoDMaster a pre-requisite, and to ProfilePlus (for PDIS0400).
- Access to JD Edwards can be through **screen-sharing** with the ability to run data browser and required reports & inquiries using the ALLOut menu program (form WAOS0001B).
  - The customer may choose to monitor the audit activity at the customer's discretion.

Standard Checklist

Identify Potential Usage

- Get full list of User profiles within system
- 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 lists and security

Identify Actual Usage

- Review modules in use (P99410 shows additional features)
- 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
- Remove redundant user profiles