JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

AUD1 - 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)

AUD2 - 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

AUD3 – JDE Compliance Assessments:

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

B – Oracle User Licensing for JD Edwards

AUD4 – 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 Security Assessments (AUD1A):

High-level Security Review
(using Read-Only Data Browser Access)

Synopsis:

Your JD Edwards (security) risk exposure – an executive briefing compiled by ALLOut

"Get clarity on your risk exposure from the industry's leading specialist JD Edwards security company"

High-level Security Review

Scope and Deliverable

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 audit is intended to support internal decision-making.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session - **with access to your system** to use Data Browser
- One 3-hour session - to analyze **collected information** (no system access is required)

Key Considerations

- The assessment does **not** require a subscription to any ALLOut product.
- Access to JD Edwards can be through **screen-sharing** with the ability to use Data Browser (with access to view data in all tables) only.
  - The customer may choose to monitor the audit activity at the customer's discretion.
- Data **confidentiality** can be protected through our NDA or your NDA for the engagement.

Standard Checklist

Identify Current Access (using Data Browser)

- Determine Security Model
  - Effective 'Deny All' vs Hyper Exit Security
  - Action Code vs Application security (read-only vs update permissions)
  - Fastpath access
  - Row security used (Company, Business Unit, Address Book)
  - Publicly accessible programs
  - User environment access exceptions
  - Menu Filtering vs Processing Option security vs Task 'blind execution' setup
  - Use of multiple Role assignments and the Role Chooser
  - Role environment access managed at Role or User level
- UDO development access

Assess Risk Exposure - to include findings:

- If excessive access to key programs
- If privileged User (IT) profile exposure (*ALL Access)
- If key Segregation of Duties rules are breached

Suggest Remediation and Best Practices

- Security 'Deny All'
  - Security change control
- Use of multiple Role assignments and Role Chooser
  - Role assignment change control and approval
- Menu Filtering (for version control)
- Segregation of Duties remediation vs mitigation
- Password Policy

ALLOut Security

JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

AUD1 - 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)

AUD2 - 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

AUD3 – JDE Compliance Assessments:

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

B – Oracle User Licensing for JD Edwards

AUD4 – 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 Security Assessments (AUD1B):

Comprehensive SoD & System Access Assessment
(using exported copy of your Security Data)

Synopsis:

Your SoD & JD Edwards access risk exposure – an executive briefing compiled by ALLOut

"Get clarity on your risk exposure from the industry's leading specialist JD Edwards security company"

Comprehensive SoD & System Access Assessment

Scope and Deliverable

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

Engagement Length

Four 3-hour sessions (12 hours) - using your exported data to prepare the assessment

Key Considerations

- The assessment does **not** require a subscription to any ALLOut product.
- A **copy** of your security data is required – i.e., the data within the tables:
  - Users - F0092, F98OWSEC and **optionally** F0101 (for User descriptions)
  - Roles - F0092, F00926
  - Environment access - F00941, F0093
  - Role Relationships and security - F95951, F00950 and **optionally** F00950W (to include UDO development if JDE 9.2)
  - Menu Filtering (this is **optional** to include menu access) - F9000, F9001, F9006
- The data can be exported in any convenient format including **CSV**.
- Data **confidentiality** can be protected through our NDA or your NDA for the engagement.

Standard Checklist

Determine Security Model - as in AUD1A

Run Reports to Identify Risk - Segregation of Duties

- Load ALLOut SoDMaster Rules and Critical Program Lists
- Run active User SoD report (PCML0600)
  - Run within-Role SoD report (PCML0600)

Run Reports to Identify Risk - User Access Review

- Run active User Critical Access report (PCML0600)
  - Run Role Critical Access report (PCML0600)
- Run inactive profile exposure (PCML0930)

Suggest Remediation and Best Practices

- Security strategy:
  - Security 'Deny All' vs Open model
  - Security access change control
  - Menu Filtering (for version control)
- Use of multiple Role assignments and Role Chooser
  - Role assignment change control and approval
- Segregation of Duties remediation vs mitigation
- Password policy