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)

ALLOut Product Verification: (VERIFY1A)

JDE Access (Changes) Auditing Verification

Synopsis:

A 3-hour engagement to verify the audit and review processes around your JD Edwards system access and change control – an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

JD Edwards Access (Changes) Auditing Verification

Scope and Deliverable

The audit deliverable is an ALLOut-certified verification of the auditing data capture of your JD Edwards system access and change controls, and the extent to which your audit processes can be effective.

The objective is to provide management with concise information and to identify any potential improvements to current auditing activities.

No changes will be made to your system – all reports will be made in proof mode only.

Engagement Length

One 3-hour session (3 hours)

- One 3-hour session with **access to your system** to run ALLOut reports and inquiries and read-only access to configuration screens.

Key Considerations

- The verification assumes a subscription to ALLOut software.
- Access to JD Edwards can be through **screen-sharing** with the ability to run required reports & inquiries and verify configuration using the ALLOut menu program (PAOS0001).
  - The customer may choose to monitor the audit activity at the customer's discretion.

Standard Checklist

Verify Audit Data Capture

- Verify ALLOut feature configuration
- Sample User, Role & Security changes
  - User profile creation, deprovisioning & password reset
  - Role Creation approval and environment enabling
  - Redundant profile clean-up
  - Security changes – Application and Action Code, UDOs, Menu Filtering
  - Security change control approvals (SCC) sampling
- Sample Role Assignment changes
  - Role Assignment documentation
  - Request and approval (RbAC) activity
  - Restricted role (RbAC) combination changes (Role-based SoD) and assignment activity

Verify Audit Review Processes

- Sample Access Reporting controls
  - SoD Rules and Critical Lists changes
  - Mitigating Control definitions and assignment changes
- Sample Access approval processes
  - Audit & Review Segregation of Duties
  - Audit & Review Critical Access
  - Risk Approval Reporting for Segregation of Duties
  - Risk Approval Reporting for Critical Access (Critical Programs and/or Role Assignments)

Suggest Potential Improvements to your Audit Processes

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)

ALLOut Product Verification: (VERIFY1B)

JDE Access Changes & Controls Verification
(Security & Role Change Controls Audit)

Synopsis:

A 3-hour engagement to verify your JD Edwards system access change controls – an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

JD Edwards Access Changes & Controls Verification

(Security and Role Change Controls Audit)

Scope and Deliverable

The audit deliverable is an ALLOut-certified verification of your current system access (security and role) change control processes, and the extent to which your change control processes can be effective.

The objective is to provide management with concise information and to identify any additional controls that could prevent unwanted system access.

No changes will be made to your system – all reports will be made in proof mode only.

Engagement Length

One 3-hour session (3 hours)

- One 3-hour session with **access to your system** with read-only access to configuration screens

Key Considerations

- The verification assumes a subscription to ALLOut software
- Access to JD Edwards can be through **screen-sharing** with the ability to run required reports & inquiries and verify configuration using the ALLOut menu program (PAOS0001)
  - The customer may choose to monitor the audit activity at the customer's discretion

Standard Checklist

Verify Access Change Controls

- Sample User provisioning and de-provisioning
  - Inactive profile exposure
  - Password strength and change frequency
- Sample Role Ownership
  - Naming convention if any for update, inquiry & data roles
  - Environment access changes
- Sample Role Assignment controls
  - Role Restrictions – Privileged Role ownership (Approver Lists)
  - Role Restrictions – Manager staff ownership (Approver Lists)
  - Role Request & Approval
  - Segregation of Duties prevention
  - Segregation of Duties mitigation
  - Role Assignment documentation standards
- Sample Role (and User) Security Change Controls
  - Change Control Approver Lists
  - Security & Role Assignment Promotion
  - User Acceptance Testing Approval process
  - Segregation of Duties Validation process
  - *PUBLIC and *ALL security changes

Suggest Potential Improvements to your Access Change Control Processes

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)

ALLOut Product Verification: (VERIFY1C)

Post-Upgrade/Install Verification
(ALLOut Functionality Audit)

Synopsis:

A 6-hour engagement to verify your implemented and potential usage of ALLOut functionality – an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

ALLOut for E1: Post-Upgrade/Install Verification
(ALLOut Functionality Audit)

Scope and Deliverable

The audit deliverable is an ALLOut-certified verification of previously implemented ALLOut features – typically following an implementation or software upgrade.

The objective is to provide management with concise information and to identify any features that could be easily adopted by your business to provide value without additional investment.

No changes will be made to your system – all reports will be made in proof mode only.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session(s) 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 verification can be conducted in **either** PY (before software promotion) or PD
  - If testing is in PY, configuration can be compared to PD (if access is available)
  - If testing is in PD, configuration can be compared to previous PDFs (if supplied)
- Access to JD Edwards can be through **screen-sharing** with the ability to run required reports & inquiries and verify configuration using the ALLOut menu program (PAOS0001)
  - The customer may choose to monitor the audit activity at the customer's discretion

Standard Checklist

Verify implemented ALLOut features

- System Access Change Controls
  - Role Assignment Controls
  - Multiple Role Security (and optionally Menu Filtering) Fix-Merge (RMUR0400/200)
  - Role Security, Menu Filtering, and/or Assignment Promotion (RMUR0403/203/603)
- Reporting configuration
  - SoD Rule Definition & Application best-practice (RCML0500)
  - User Access Review (of Program Access) best-practice (RCML0500)
  - User Access Review (of Role Assignments) best-practice (RCML0961)
  - User Access Review (of Company Access) best-practice (RCML0550)
- Risk Mitigation and Approval controls
  - Audit History Capture and Review controls (RCML0251)
  - SoD/Access Mitigating Controls (PCML0945)
  - Risk Approval (PCML0880)
- Audit History Review processes
  - Security Change Review (PCML0255)
  - SoD Breach History (PCML0601)
  - Critical Access History (PCML0601)