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)

ALLOut Product Verifications: (AUD4A)

JDE Access (Changes) Auditing Verification

Synopsis:

Your JD Edwards access auditing (implemented and potential) – an executive briefing compiled by ALLOut

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

JD Edwards Access (Changes) Auditing Verification

Scope and Deliverable

The audit deliverable is an ALLOut-certified verification of your current access audit and review processes, and the extent to which security changes may be effectively audited.

The objective is to verify the effectiveness of current access audit or review processes and identify any potential improvements. The audit is intended to support internal compliance and ensure readiness for external audits.

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 Current Auditing

- Verify ALLOut feature configuration
- Sample User, Role & Security changes (PCML0250)
  - User profile creation, deprovisioning & password reset
  - Role Creation approval and environment enabling
  - Redundant profile clean-up (PDIS0400)
  - Security changes – Application and Action Code, UDOs, Menu Filtering
  - Security change control approvals (SCC) sampling
- Sample Role Assignment changes (PCML0250)
  - Role Assignment documentation (PCML0961)
  - Request and approval (RbAC) activity
  - Restricted role (RbAC) combination changes (Role-based SoD) and assignment activity
- Sample Access Reporting controls (PCML0250)
  - SoD Rules and Critical Lists changes
  - Mitigating Control definitions and assignment changes
- Sample Access approval processes (PCML0601)
  - 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 Remediation if processes partially implemented

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)

ALLOut Product Verifications: (AUD4B)

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

Synopsis:

Your JD Edwards Security change controls (implemented and potential) – an executive briefing compiled by ALLOut

"Get clarity on your risk exposure from the industry's leading 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.

The objective is to verify the effectiveness of current ALLOut change controls and identify any potential improvements. The audit is intended to support internal compliance and ensure readiness for external audits.

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 Current Controls (using ALLOut feature configuration)

- Verify User provisioning and de-provisioning
  - Run inactive profile exposure (PCML0930)
  - Password strength and change frequency
- Verify Role Ownership
  - Naming convention if any for update, inquiry & data roles
  - Environment access changes
- Verify Role Assignment controls
  - Privileged Role – Assignment access ownership (Approver Lists)
  - Manager – Assignment access ownership for manager's staff (Approver Lists)
  - Role Restrictions
  - Role Request & Approval
  - Segregation of Duties prevention, remediation & mitigation process
  - Role Assignment documentation standards
- Verify Role (and User) Security Change Controls
  - Change Control Approver Lists
  - Security & Role Assignment Promotion
  - User Acceptance Testing Approval process
  - Segregation of Duties prevention, remediation & mitigation process
  - *PUBLIC and *ALL security changes

Suggest Remediation if processes partially implemented

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)

ALLOut Product Verifications: (AUD4C)

Post-Upgrade/Install Verification
(ALLOut Functionality Audit)

Synopsis:

Your ALLOut functionality (implemented and potential) – an executive briefing compiled by ALLOut

"Get clarity on your risk exposure from the industry's leading 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 your ALLOut implementation – typically following an implementation or upgrade.

The objective is to verify the effectiveness of previously implemented features and highlight any features that could provide additional value specific to the Customer's current circumstances. The audit is intended to support internal compliance and decision-making,

Engagement Length

Two 3-hour sessions (6 hours)

- One to two 3-hour session(s) with **access to your system** to run ALLOut reports and inquiries and read-only access to configuration screens.
  - The number of sessions depends on the features to verify.
- 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.
  - Configuration - if testing is in PY, PD configuration can be used if PD access is available.
  - Processing Options – previous PDFs can be used to verify required processing options.
  - Test roles should be created **beforehand** to facilitate testing.
- 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 previously implemented ALLOut features are active (as chosen by Customer)

- Verify 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)
- Verify 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)
- Verify Risk Mitigation and Approval controls
  - Audit History Capture and Review controls (RCML0251)
  - SoD/Access Mitigating Controls (PCML0945)
  - Risk Approval (PCML0880)
- Verify Audit History Review processes
  - Security Change Review (PCML0255)
  - SoD Breach History (PCML0601)
  - Critical Access History (PCML0601)