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 (AUD2A):

InfoSec Security Assessment
(for ISO/IEC within JD Edwards)

Synopsis:

Your Information Security framework within JD Edwards – an executive briefing compiled by ALLOut

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

InfoSec Security Assessment (for ISO/IEC)

Scope and Deliverable

The audit deliverable is an ALLOut-certified assessment of the effectiveness of your current JD Edwards security and system access controls including change management and monitoring.

The objective is to assess the completeness of existing policies and identify any potential improvements. The audit is intended to prepare the ground for Segregation of Duties initiatives, support internal compliance and ensure readiness for external audits.

Standard Engagement Length

Three 3-hour sessions (9 hours)

- Two 3-hour sessions with **access to your system** to view JD Edwards security information.
- One 3-hour session - to analyze **collected information** (no system access is required)

Key Considerations

- The assessment assumes a subscription to ALLOut software.
- Access to JD Edwards can be through **screen-sharing** with the ability to run inquiries, verify ALLOut configuration using menu program PAOS0001 and use Data Browser.
  - The customer may choose to monitor the audit activity at the customer's discretion.

Standard Checklist

Identify Current Access (using Data Browser as per AUD1A)

- Determine Security Model including UDO development access
- Determine Segregation of Duties policies

Assess System Access

- Verify privileged (IT) account access vulnerability
  - Access to production not available (enabled by separate roles)
  - JD Edwards accounts separate from database accounts (F98OWPU)
  - Developer (OMW) access limited to privileged accounts
- Verify Business User account access vulnerability
  - Non-prod environment access limited to privileged and/or minimal test accounts
  - Inactive or leaver accounts disabled (if F9312 capturing information)
  - System Deny All in place with Application and Action Code
  - Menu Filtering or Version-level and Menu security
  - Redundant security data cleaned-up (PDIS0150)
  - Application security (critical program) change controls (config)
  - Role assignment documentation and controls (config)
- Verify System Access and Ownership
  - Password policy and change frequency (config)
  - Segregation of Duties review, remediation & mitigation
  - Role update controls and ownership and Business Manager ownership (PCML0610)

Assess Software Development & Operational Control

- Custom software change management requirements (F9860)
- Security Change History (F9312) enabled
- Application Access History (F98902 & F98911) enabled

Suggest Remediation and Best Practices (as per AUD1A)

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 (AUD2B):

Segregation of Duties: Risk Analysis

Synopsis:

Your Segregation of Duties risk exposure – an executive briefing compiled by ALLOut

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

Segregation of Duties Risk Analysis

Scope and Deliverable

The audit deliverable is an ALLOut-certified assessment of your current Segregation of Duties exposure within your JD Edwards system based on a full SoD report and relevant analysis of underlying security.

The objective is to identify critical areas of risk and guide effective mitigation efforts with suggestions of current remediation and mitigation strategies available. The audit is intended to support internal compliance and ensure readiness for external audits.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session with **access to your system** to run ALLOut reports and inquiries.
- 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 requires a subscription to ALLOut **Risk Reporting** and for SoD Rules and Critical Lists to be uploaded **beforehand**. (The full set of rules and lists can be uploaded from the ALLOut SoDMaster product or customized as preferred by the customer).
- Access to JD Edwards can be through **screen-sharing** with the ability to run ALLOut reports and inquiries using the ALLOut menu program (form WAOS0001B).
  - The customer may choose to monitor the audit activity at the customer's discretion.

Standard Checklist

Run Reports to Identify Risk

- Review current SoD rules (PCML0260)
  - Verify Critical Program Lists used by Rules
  - Verify no custom programs exist, or that Lists include custom programs
  - Verify SoD Mitigating Controls (if any)
- Run User SoD Report for active Users (PCML0600)
  - Run Role SoD Report for within-Role conflicts (PCML0600)

Assess Risk Exposure - to include findings:

- Privileged User (IT) profile exposure
- Rule breach analysis

Suggest Remediation and Best Practices

- Security strategy:
  - Multiple Roles & the Role Chooser
  - Deny All vs Menu Filtering with Exit security
  - User-level security exceptions
  - Publicly accessible programs
  - Fastpath access
  - Action Code vs Application security (read-only vs update permissions)
- Use of Mitigating Controls (PCML0945)

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 (AUD2C):

User Access Review: Functional (Program) Access

Synopsis:

Your Business Data vulnerability (by functional area) – an executive briefing compiled by ALLOut

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

User Access Review: Functional (Program) Access

Scope and Deliverable

The audit deliverable is an ALLOut-certified assessment of the current User (and role) access permitted to your JD Edwards system and any risk exposure resulting from that access.

The objective is to identify critical areas of risk and guide effective mitigation efforts of any excessive functional access. The audit is intended to support internal compliance and ensure readiness for external audits.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session with **access to your system** to run ALLOut reports and inquiries.
- 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 requires a subscription to (ideally) ALLOut **Risk Reporting** or to MenuPlus (if not available). If using Risk Reporting, Critical Lists should be uploaded **beforehand**. (Use ALLOut **SoDMaster** to upload All Lists as supplied or customize as preferred).
- Access to JD Edwards can be through **screen-sharing** with the ability to run ALLOut reports and inquiries using the ALLOut menu program (form WAOS0001B).
  - The customer may choose to monitor the audit activity at the customer's discretion.

Standard Checklist

Run Reports to Identify Risk (if using Risk Reporting)

- Report Critical Lists in use (PCML0260)
  - Verify no custom programs exist, or that Lists include custom programs
  - Verify access Mitigating Controls (if any)
- Run User Critical Access report (PCML0600)
  - Run Role Critical Access report (PCML0600)
- Run inactive profile exposure (PCML0930 within ProfilePlus if available)

Run Reports to Identify Risk (if using MenuPlus)

- Verify current Menu Task Views used (Data Browser of F9000 type 00)
  - Verify Menu Filtering always exists (PDIS0400 within ProfilePlus if available)
- Run User Critical Access report (PCML0725)
  - Run Role Critical Access report (PCML0725)

Assess Risk Exposure and Suggest Remediation

- Privileged User (IT) profile exposure
- Inactive profile exposure
- Security strategy:
  - Multiple Roles & the Role Chooser
  - Deny All vs Menu Filtering with Exit security
  - Action vs Application security (read vs update permissions)
  - User-level security exceptions; Publicly accessible programs; Fastpath access
- Use of Mitigating Controls (PCML0945)

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 (AUD2D):

User Access Review: Company (Data) Access

Synopsis:

Your Business Data vulnerability (by company access) – an executive briefing compiled by ALLOut

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

User Access Review: Company (Data) Access

Scope and Deliverable

The audit deliverable is an ALLOut-certified assessment of the current User (and role) access permitted to your JD Edwards system in a multi-company environment where access to each company's data needs to be controlled independently.

The objective is to identify critical areas of non-compliance and guide effective mitigation efforts of any unauthorized access. The audit is intended to support internal compliance.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session with **access to your system** to run ALLOut reports and inquiries.
- 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 requires a subscription to ALLOut **Risk Reporting** and **SecurityPlus**.
- Access to JD Edwards can be through **screen-sharing** with the ability to run ALLOut reports and inquiries using the ALLOut menu program (form WAOS0001B).
- The customer may choose to monitor the audit activity at the customer's discretion.

Standard Checklist

Run Reports to Identify Risk

- Verify companies used (data browser or P0010)
  - Verify row security exists for key tables and data items (PAOS0950)
- Run User access to company report (PCML0650)
  - Run Role access to company report (PCML0650)
- Run User access to Business Units report (PCML0650)
  - Run Role access to Business Units report (PCML0650)
- Run inactive profile exposure (PCML0930 within ProfilePlus if available)

Assess Risk Exposure - to include findings:

- Privileged User (IT) profile exposure
- Inactive profile exposure

Suggest Remediation and Best Practices

- Security strategy:
  - Multiple roles & the Role Chooser
  - *ALL file "Deny All" vs specific tables
  - Read-Only (View) vs update permissions
  - User-level security exceptions
  - Inclusive Vs Exclusive Row security
- Missing Tables
  - Missing Data items