ALLOut Security

JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

ASSESS – JDE Security Assessments
(**without** installing ALLOut software):

A – High-Level Security Assessment
(using your JDE system without ALLOut)

B – High-Level Security Assessment
(of exported copy of your security data)

C – SoD & User Access Assessment
(of exported copy of your security data)

REVIEW - JDE Access Reviews
(**using** your installed ALLOut software):

A – JD Edwards Security Essentials
(for InfoSec & ISO/IEC Standards)

B – Segregation of Duties Risk Review
(Breaches & mitigating Controls)

C – User Access Review
(of Functional and Data Access)

COMPLY – JDE Compliance Reviews:
(**using** your installed ALLOut software):

A – Personal Data in JDE
(Regulatory Risk for GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – JDE Access Control Verifications:
(**of your** installed ALLOut software):

A – JD Edwards Security Change Controls

B – ALLOut Functionality Effectiveness
(Post-Install/Upgrade)

JD Edwards Access Review (REVIEW-A)

JD Edwards Security Essentials
for InfoSec & ISO/IEC standards
(using installed ALLOut software on your JDE System)

Synopsis:

A 6-hour engagement to assess the effectiveness of your JD Edwards Information Security framework and identify practical remediation to risk exposure – an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

For more information visit www.alloutsecurity.com or email info@alloutsecurity.com

JD Edwards Security Essentials for InfoSec & ISO/IEC standards

(using installed ALLOut software on your JDE System)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified assessment of the effectiveness of your current JD Edwards security and system access controls including change management and monitoring. No changes will be made to your system – this engagement is to conduct an audit.

The scope is to assess the effectiveness of the existing approach and identify potential improvements. The objective is to provide documentary evidence to satisfy external audit requirements.

Engagement Length

Three 3-hour sessions (6 hours)

- One 3-hour session with access to **your JDE system using Microsoft Teams** screen-sharing.
- One 3-hour session - to analyze **collected information** (further system access is not required).

Key Considerations

- If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
- An active ALLOut product subscription is required. **Version 4.1** is advised.
  - Access to your JD Edwards is to run ALLOut reports and inquiries using the ALLOut menu program (form WAOS0001B), verify ALLOut configuration using menu program PAOS0001 and use Data Browser.

Audit Checklist

Determine Current Access Controls

- Verify privileged (IT) account access vulnerability
  - Developer Access to production is not available (enabled by separate roles with F0093)
  - JD Edwards accounts are separate from database accounts (F98OWPU)
  - Access to OMW (P98220) is limited (F00950)
  - Non-prod environment access limited to privileged accounts (F0093)
- Verify Business User account access vulnerability
  - System Deny All in place with Application and Action Code (F00950)
  - Menu Filtering or Version-level and Menu security are in place (F00950 & F9006)
  - Databrowser and Fastpath restrictions are in place (F00950)
  - Redundant security data being cleaned up when Users deleted (F9312)
  - UDO development access is restricted for orchestrator and query (F00950W)
  - User accounts are being disabled or deleted consistently (What is Staff turnover?) (F9312)
- Verify Access Ownership
  - Segregation of Duties rules & mitigations (ALLOut configuration with F9312)
  - Role assignment documentation and controls (ALLOut configuration with F9312)
  - Security change controls (ALLOut configuration with F9312)
  - Password policy and change frequency (JDE configuration)
  - Role ownership and Business Manager ownership (ALLOut configuration with F9312)

Verify Usage History Capture

- Security Login History (F9312) enabled
- Object Usage Tracking (F989998/9) enabled

Assess Risk Exposure and Suggest Remediation

JD Edwards Security Audits

(ALLOut-Certified)

Your Choice of Security Audits

ASSESS – JDE Security Assessments
(**without** installing ALLOut software):

A – High-Level Security Assessment
(using your JDE system without ALLOut)

B – High-Level Security Assessment
(of exported copy of your security data)

C – SoD & User Access Assessment
(of exported copy of your security data)

REVIEW - JDE Access Reviews
(**using** your installed ALLOut software):

A – JD Edwards Security Essentials
(for InfoSec & ISO/IEC Standards)

B – Segregation of Duties Risk Review
(Breaches & mitigating Controls)

C – User Access Review
(of Functional and Data Access)

COMPLY – JDE Compliance Reviews:
(**using** your installed ALLOut software):

A – Personal Data in JDE
(Regulatory Risk for GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – JDE Access Control Verifications:
(**of your** installed ALLOut software):

A – JD Edwards Security Change Controls

B – ALLOut Functionality Effectiveness
(Post-Install/Upgrade)

JD Edwards Access Review (REVIEW-B)

Segregation of Duties Risk Review: Breaches & mitigating Controls

(using installed ALLOut software on your JDE System)

Synopsis:

A 6-hour engagement to assess your JD Edwards Segregation of Duties risk exposure and identify practical remediation – an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

Segregation of Duties Risk Review: Breaches & mitigating Controls

(using installed ALLOut software on your JDE System)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified assessment of your current Segregation of Duties exposure within your JD Edwards system, using identified rules with relevant analysis of underlying security. No changes will be made to your system – this engagement is to conduct an audit.

The scope is to identify critical areas of risk and suggest effective remediation and mitigation strategies. The objective is to provide documentary evidence to satisfy external audit requirements.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session - with access to **your JDE system using Microsoft Teams** screen-sharing.
- One 3-hour session - to analyze **collected information** (further system access is not required).

Key Considerations

- If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
- An active ALLOut product subscription is required. **Version 4.1** is advised.
  - Access to your JD Edwards is to run ALLOut reports and inquiries using the ALLOut menu program (form WAOS0001B).
  - Your preferred SoD Rules and supporting Critical Lists must be uploaded **beforehand by you** (from ALLOut **SoDMaster** or from another source as preferred).
  - If no pre-loaded Rules are found, we will load 4 ‘sample’ Rules (and supporting Lists) for you.

Audit Checklist

Determine Current Access

- Review current SoD rules in use and fit for purpose
  - Verify Critical Program Lists used by Rules are not missing standard JDE programs
  - Verify no custom programs exist, or that Lists include custom programs
  - Apply SoD Mitigating Controls (if any)
- Run User SoD Report for active Users
  - Run Role SoD Report to identify within-Role conflicts

Assess Risk Exposure and Suggest Remediation

- Rule breach assessment
  - Privileged User (IT) profiles vs Business Users
- 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 Deny All (default permissions are read-only or update capable)
- Use of Mitigating Controls to effectively control excessive access

ALLOut Security

JD Edwards Security Audits

(ALLOut-Certified)

Your Choice of Security Audits

ASSESS – JDE Security Assessments
(**without** installing ALLOut software):

A – High-Level Security Assessment
(using your JDE system without ALLOut)

B – High-Level Security Assessment
(of exported copy of your security data)

C – SoD & User Access Assessment
(of exported copy of your security data)

REVIEW - JDE Access Reviews
(**using** your installed ALLOut software):

A – JD Edwards Security Essentials
(for InfoSec & ISO/IEC Standards)

B – Segregation of Duties Risk Review
(Breaches & mitigating Controls)

C – User Access Review
(of Functional and Data Access)

COMPLY – JDE Compliance Reviews:
(**using** your installed ALLOut software):

A – Personal Data in JDE
(Regulatory Risk for GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – JDE Access Control Verifications:
(**of your** installed ALLOut software):

A – JD Edwards Security Change Controls

B – ALLOut Functionality Effectiveness
(Post-Install/Upgrade)

JD Edwards Access Review (REVIEW-C)

User Access Review

of Functional and Data Access

(using installed ALLOut software on your JDE System)

Synopsis:

A 6-hour engagement to assess the vulnerability of your sensitive JD Edwards business data, by business process, and identify practical remediation
– an executive briefing compiled by ALLOut

“Get clarity from the specialist JD Edwards security company”

User Access Review of Functional and Data Access

(using installed ALLOut software on your JDE System)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified assessment of the User (and role) access that is currently permitted within your JD Edwards system and any risk exposure resulting from that access. No changes will be made to your system – this engagement is to conduct an audit.

The scope is to identify critical areas of risk and suggest effective mitigation of any excessive access. The objective is to provide documentary evidence to satisfy external audit requirements.

Engagement Length

Two 3-hour sessions (6 hours)

- One 3-hour session - with access to **your JDE system using Microsoft Teams** screen-sharing.
- One 3-hour session - to analyze **collected information** (further system access is not required).

Key Considerations

- If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
- An active ALLOut product subscription is required. **Version 4.1** is advised.
  - Access to your JD Edwards is to run ALLOut reports and inquiries using the ALLOut menu program (form WAOS0001B).
  - Critical Program Lists must be uploaded **beforehand by you** (from ALLOut **SoDMaster** or from another source). If no pre-loaded Lists are found, we will load 5 'sample' Lists for you.
- The audit can be based on **either** program access **or** menu access **or** company (row security). Unless explicitly requested, the audit will be based on Critical Program access.

Audit Checklist

Determine Current Access

- If reporting program or menu access, verify Critical Lists exist.
  - Verify no custom programs exist (F9860), or Lists include custom programs (Configuration)
- If reporting menu access, verify Task Views used (F9000 type 00) & Menu Filtering exists
- If reporting company access, verify active companies (F0010)
- Run User Access report
  - Run Role Access report – verifying Role access matches Role description

Assess Risk Exposure and Suggest Remediation

- Critical process access assessment
  - Privileged User (IT) profiles vs Business Users
  - Use of Mitigating Controls to effectively control excessive access
  - Multiple Roles & the Role Chooser
  - User-level security exceptions
- If reporting program or menu access, assess Security strategy:
  - Deny All vs Menu Filtering with Exit security,
  - Fastpath access; Publicly accessible programs
  - Action Code Deny All (default permissions are read-only or update capable)
- If reporting company data access, assess impact of Exclusive vs Inclusive (see White Paper)
  - Missing *Public security; Applying *ALL vs missing tables; Missing Data items (MCU*)