Assess Risk Exposure — Review & Verify Risk Controls

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)

JDE Access Controls Verification (VERIFY-A)

JD Edwards Security Change Controls
(of installed ALLOut software on your JDE System)

Synopsis:

A 6-hour engagement to verify your JD Edwards system access change controls (preventative and post-change review) – 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 Change Controls

(of installed ALLOut software on your JDE System)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified verification of your change controls and audit review processes to ensure effective oversight of ongoing changes to security access within JD Edwards. No changes will be made to your system – this engagement is to conduct an audit.

The scope is to verify the effectiveness of the preventative controls and auditing procedures already implemented to stop unwanted access and suggest any potential improvements. 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 and verify configuration using the ALLOut menu program (PAOS0001).

Audit Checklist

Verify configured Audit Data Capture

- User/Role changes: Active controls vs Update log
  - User profiles – including Password strength and change frequency
  - Role Creation – including environment access changes
- Security changes – Active controls vs Update log
  - Application and Action Code, UDOs, Menu Filtering *PUBLIC and *ALL changes

Verify (preventative) Access Change Processes

- Role Assignment changes: Active controls vs update log
  - Role Assignment documentation
  - Request and approval (RbAC)
  - Role Restrictions (RbAC) – Role-based Segregation of Duties and allowed exceptions
  - Role Restrictions (RbAC) – Team Manager and/or Role Owner changes (Approver Lists)
- Security change control (SCC) – Validation and Approval activity
  - Security & Role Assignment Promotion

Verify (post-change) Access Review Processes

- Access Reporting controls - Active controls vs update log
  - Segregation of Duties Rules and Critical Lists
  - Mitigating Control definitions and assignments
- Access Review processes
  - Audit & Review – of Segregation of Duties breaches
  - Audit & Review – of Critical Program Access

Validate Existing Process Effectiveness and Advise any necessary Remediation

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)

JDE Access Controls Verification (VERIFY-B)

ALLOut Functionality Effectiveness (Post-Install/Upgrade)

(of installed ALLOut software on your JDE System)

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 Functionality Effectiveness (Post-Install/Upgrade)

(of installed ALLOut software on your JDE System)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified verification of previously implemented ALLOut features – typically following the product implementation or software upgrade. No changes will be made to your system – this engagement is to conduct an audit.

The scope is to verify the configuration of implemented features and briefly describe their purpose and effect on your JD Edwards system with the objective to provide documentary evidence to satisfy external audit requirements. ALL reports will be run in proof mode only, so no data is updated.

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 and verify configuration using the ALLOut menu program (PAOS0001).
- 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)

Audit 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)

Validate Existing Process Effectiveness and Advise any necessary Remediation