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 Security Assessment (ASSESS-A)

High-level Security Assessment
(using your JDE system without ALLOut)

Synopsis:

A 6-hour engagement to identify JD Edwards security risk exposure and identify practical remediation
– an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

High-level Security Assessment
(using your JDE system without ALLOut)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified assessment of the current access 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 any critical areas of risk, provide an opinion on likely Segregation of Duties exposure, and make workable suggestions to guide effective access controls. The objective is to support effective management decision-making.

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.
- **No ALLOut software is used.**
  - Access to your JD Edwards system is to use Data Browser.
- Your data **confidentiality** can be protected through our NDA or your NDA.

Audit Checklist

Identify Current Access (using Data Browser)

- Determine Security Model
  - Effective 'Deny All' vs Hyper Exit Security
  - Action Code vs Application security (read-only vs update permissions)
  - Fastpath access
  - Row security used (Company, Business Unit, Address Book)
  - Publicly accessible programs
  - User-level access exceptions
  - Menu Filtering vs Processing Option security vs Task 'blind execution' setup
  - Use of multiple Role assignments and the Role Chooser
  - Role environment access managed at Role or User level
- UDO development access

Assess if excessive Risk Exposure:

- Business User access (to key programs)
- Privileged User (IT) profile exposure

Suggest Remediation and Best Practices

- Security 'Deny All'
  - Security change control
- Use of multiple Role assignments and Role Chooser
  - Role assignment change control and approval
- Menu Filtering (for version control)
- Segregation of Duties remediation vs mitigation
- Password Policy

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 Security Assessment (ASSESS-B)

High-level Security Assessment
(of exported copy of your Security Data)

Synopsis:

A 6-hour engagement to identify JD Edwards security risk exposure and identify practical remediation
– an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

High-level Security Assessment

(of exported copy of your Security Data)

Audit Scope and Deliverable

The deliverable is an ALLOut-certified assessment of the current access permitted within your JD Edwards system and any risk exposure resulting from that access. No access is required to your system – the audit will be conducted over the security data that you provide us with.

The scope is to identify any critical areas of risk, provide an opinion on likely Segregation of Duties exposure, and make workable suggestions to guide effective access controls. The objective is to support effective management decision-making.

Engagement Length

Two 3-hour sessions (6 hours) - using your exported data to prepare the assessment.

Key Considerations

An exported copy of your security data <u>is</u> required.

- **No ALLOut software is used.**
- **Access to your JD Edwards system is <u>not</u> required.**
- Please email us (in CSV format) a copy of the data within the following tables:
  - User Profiles - F0092, F98OWSEC and **optionally** F0101 (for User descriptions)
  - Role Profiles - F0092, F00926
  - Environment access - **optionally** F0093
  - Role Relationships and security - F95951, F00950 and **optionally** F00950W (to include UDO development if JDE 9.2)
  - Menu Filtering (this is **optional** to include menu access) - F9000, F9001, F9006
- Your data **confidentiality** can be protected through our NDA or your NDA.

Audit Checklist

As in ASSESS1A – ALLOut software will not be used.

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 Security Assessment (ASSESS-C)

SoD & User Access Assessment: Procurement Module Insights
(of exported copy of your Security Data)

Synopsis:

An 18-hour engagement to identify your JD Edwards access and Segregation of Duties risk exposure, and identify practical remediation
– an executive briefing compiled by ALLOut

"Get clarity from the specialist JD Edwards security company"

SoD & User Access Assessment: Procurement Module Insights

(of exported copy of your Security Data)

Audit Scope and Deliverable

The deliverable is a comprehensive ALLOut-certified assessment of the current access to Procurement functionality within your JD Edwards system and any risk exposure resulting from that access. No access is required to your system – the audit will be conducted over the security data that you provide us with.

The scope is to identify any possible Segregation of Duties risk and guide effective mitigation efforts. The reports provided use ALLOut's best-practice Rule and List set (validated for standard JD Edwards Procurement software) to show the impact of your current security.

The objective is to support effective management decision-making. For an audit over all JD Edwards modules, install the ALLOut-for-E1 software onto your system, before requesting an ASSESS2 audit.

Engagement Length

Six 3-hour sessions (18 hours) - using your exported data to prepare the assessment.

Key Considerations

An exported copy of your security data is required.

- **No ALLOut product subscription is required.**
- **Access to your JD Edwards system is not required.**
- Please email us (in CSV format) a copy of the data within the following tables:
  - User Profiles - F0092, F98OWSEC and **optionally** F0101 (for User descriptions)
  - Role Profiles - F0092, F00926
  - Environment access - **optionally** F0093
  - Role Relationships and security - F95951, F00950 and **optionally** F00950W (to include UDO development if JDE 9.2)
  - Menu Filtering (this is **optional** to include menu access) - F9000, F9001, F9006
- Your data **confidentiality** can be protected through our NDA or your NDA.

Audit Checklist

Assess if excessive Risk Exposure:

- Run Segregation of Duties Reports - for Procurement (JD Edwards Product Code 43)
  - Load ALLOut SoDMaster Rules for Product 43 and all required Critical Program Lists
  - Run active User SoD report
  - Run within-Role SoD report
- Run Access Review Reports - for Procurement (JD Edwards Product Code 43)
  - Load ALLOut SoDMaster Critical Program Lists for Product 43
  - Run active User Critical Access report
  - Run standalone-Role Critical Access report

Suggest Remediation and Best Practices