JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

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

A –Security Policies & Access Assessment
(using our Audit Analysis AI Tool on exported copy of your security data)

B –Security Policies Only Assessment
(using JDE Data Browser on your system)

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

A – Security Policies & Controls Review
(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 JD Edwards
(Regulatory Risk with GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – ALLOut Control Verifications:
(validating **your** installed ALLOut software):

A –ALLOut Product Usage
(Making the Most of ALLOut)

B – Security Change Mgmt. in JD Edwards
(Preventing Unauthorized Access.)

C – Access Change Auditing in JD Edwards
(Detecting Unauthorized Access.)

JD Edwards Security Assessments (ASSESS-A)

Security Policies & Access Assessment

(using our Audit Analysis AI Tool on an exported copy of your security data)

Synopsis:

Identify JD Edwards security policies and access control framework and highlight any resulting risk exposure

"Get clarity from the specialist JD Edwards security company"

Security Policies & Access Assessment

(using our Audit Analysis AI Tool on an exported copy of your security data)

Key Features

Deliverable: An ALLOut-certified report providing a comprehensive assessment of your current JD Edwards security policies and access control framework, together with a high-level assessment of the current access permitted within your JD Edwards system, and the risk exposure, evidenced by excessive access and Segregation of Duties breaches.

Approach: The audit is conducted by analyzing your **exported** JD Edwards security data using our purpose-built **Audit Analysis AI Tool**.

Objective: Support informed management decision-making prior to installing any software tool or changing your current approach to security and access management.

Recommendation: For a comprehensive audit using ALLOut-for-E1 software, install the ALLOut-for-E1 software onto your system, before requesting a REVIEW audit.

Engagement

Five Audit Credits – allocated to:

- Using our **Audit Analysis AI tool** to analyze collected information to produce your report.
- An exported copy (CSV format) of the following security tables must be emailed to us:
  - User Profiles - F0092, F98OWSEC
  - Role Profiles and Environment access - F0092, F0093
  - Role Relationships and security - F95921, F00950
  - UDO development (this is optional if JDE 9.2) - F00950W
  - Menu Filtering (tables are optional if including menu security) - F9000, F9006
- Your data confidentiality can be protected through our NDA or your NDA

Audit Coverage

Identify current Access Control Policies

- (As in ASSESS-B)

Sample for excessive Risk Exposure

- Using ALLOut sample Critical Programs and SoD Rules
  - Excessive Business User access
  - Excessive Business area access
  - Privileged User (IT) access
  - Segregation of Duties within-Role breaches
  - Segregation of Duties User-level breaches

Highlight excessive Risk Exposure

- Security 'Deny All'
- Large persona-based vs process-based Roles
- Role assignment change control and approval
- Security change auditing

JD Edwards Security Audits
(ALLOut-Certified)

Your Choice of Security Audits

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

A –Security Policies & Access Assessment
(using our Audit Analysis AI Tool on exported copy of your security data)

B –Security Policies Only Assessment
(using JDE Data Browser on your system)

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

A – Security Policies & Controls Review
(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 JD Edwards
(Regulatory Risk with GDPR, CCPA etc.)

B – Oracle User Licensing for JD Edwards

VERIFY – ALLOut Control Verifications:
(validating **your** installed ALLOut software):

A –ALLOut Product Usage
(Making the Most of ALLOut)

B – Security Change Mgmt. in JD Edwards
(Preventing Unauthorized Access.)

C – Access Change Auditing in JD Edwards
(Detecting Unauthorized Access.)

JD Edwards Security Assessments (ASSESS-B)

Security Policies Only Assessment

(using JDE Data Browser on your system)

Synopsis:

Identify JD Edwards security policies and access control framework and highlight any resulting risk exposure

"Get clarity from the specialist JD Edwards security company"

Security Policies Only Assessment

(using JD Edwards Data Browser on your system)

Key Features

Deliverable: An ALLOut-certified report providing an indicative assessment of your current JD Edwards security policies and access control framework, and the likely risk exposure resulting from those policies (excessive access and Segregation of Duties breaches).

Approach: The audit is conducted by viewing your security data using **JD Edwards Data Browser** only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Support informed management decision-making prior to installing any software tool or changing your current approach to security and access management.

Recommendation: For a comprehensive audit using ALLOut-for-E1 software, install the ALLOut-for-E1 software onto your system, before requesting a REVIEW audit.

Engagement

Two Audit Credits – allocated to:

- One 3-hour session - with 'take control' access to your system using Teams or Quick Assist - to use JD Edwards Data Browser.
  - If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - Your data confidentiality can be protected through our NDA or your NDA.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Identify Current Policies (using Data Browser):

- Business User account access vulnerabilities:
  - Effective 'Deny all' vs 'Open System' (often with Hyper Exit security)
  - Action Code 'Deny all' (read-only vs update permissions)
  - Databrowser and Fastpath restrictions
- Business User role access vulnerabilities:
  - Multiple Roles used to limit individual Role scope (and reduce maintenance overhead)
  - Role Chooser disabled or 'Deny All' enforced
  - Role environment access separated at Role or User level consistently
- Privileged (IT) account access vulnerabilities:
  - Developer Access (to P98220) restricted
  - UDO development access (for orchestrator) restricted
  - Database accounts (in F98OWPU) limited or managed consistently
- Security management vulnerabilities:
  - Publicly accessible programs is limited
  - User-level access exceptions is limited
  - Processing Option security or Task Blind Execution enforced
  - Menu Filtering or Version-level security enforced

Highlight excessive Risk Exposure