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.)

ALLOut Control Verifications (VERIFY-A)

ALLOut Product Usage
(validating installed ALLOut software)

Synopsis:

Assess current ALLOut usage, including implemented features and available functionality not currently in use

"Get clarity from the specialist JD Edwards security company"

ALLOut Product Usage

(validating installed ALLOut software on your system)

Key Features

Deliverable: An ALLOut-certified verification of current ALLOut product usage, including implemented and available features – typically following product implementation or software upgrade – to assess the security policies and controls managing access within JD Edwards.

Approach: The audit is conducted using **ALLOut reports, inquiries, configuration views** (via menu program PAOS0001), and the JD Edwards Data Browser only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Provide documentary evidence to satisfy external audit requirements.

Engagement

Two Audit Credits – allocated to:

- One 3-hour session - **with 'take control' access to your system using Teams or Quick Assist**
  - If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - ALLOut software must be pre-installed and the product license active.
  - ALLOut for E1 Version 4.1 is advised.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Review implemented ALLOut for E1/World features

- Segregation of Duties
  - SoD Breach Reporting across Multiple Systems
  - SoD Breach Mitigation
  - SoD Breach KPI tracking
- JDE Access
  - Critical Access KPI tracking
  - Inactive User Management
- Ownership & Accountability
  - Online Approval for Business Owners
- Change Monitoring
  - Audited Security, Role & User Updates
  - Audited Multiple Role Limitations (Fix-Merge with/without SRs)
  - Audited Security & Role Assignments Maintenance
  - Audited User Provisioning and De-provisioning
- Access Change Management
  - Change Control Automation: Role Assignments or Security Data Promotion
  - Role-based Segregation of Duties Prevention
  - User and/or Role Access Restrictions
  - Role Request and Approval

Review implemented ALLOut Trace features

- Privileged User & Backdoor Access Monitoring
- Named (At-Risk) Table Monitoring

Assess effectiveness of existing configuration

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.)

ALLOut Control Verifications (VERIFY-B)

Security Change Management (Risk Prevention) in JD Edwards
(validating installed ALLOut software)

Synopsis:

Assess your JD Edwards system access (preventative) change controls

"Get clarity from the specialist JD Edwards security company"

Security Change Management (Risk Prevention) in JD Edwards

(validating installed ALLOut software on your system)

Key Features

Deliverable: An ALLOut-certified verification of your security change controls, assessing whether they provide effective control over ongoing changes to security access within JD Edwards.

Approach: The audit is conducted using **ALLOut reports, inquiries and configuration views** (via menu program PAOS0001), and the JD Edwards Data Browser only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Provide documentary evidence to satisfy external audit requirements.

Engagement

Two Audit Credits – allocated to:

- One 3-hour session - **with 'take control' access to your system using Teams or Quick Assist**
- If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - ALLOut software must be pre-installed and the product license active.
  - ALLOut for E1 Version 4.1 is advised.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Review (preventative) Access Change Processes

- Maintenance Controls
  - User Data
  - Role Data
  - Security Data
- Role Assignment Documentation
  - Active controls:
- Role Assignment Request and approval (RbAC)
  - One-Step Approve=Create (without Workflow)
  - Multi-Step Approve->Create (without Workflow)
- Role Assignment Restrictions (RbAC)
  - Role-based Segregation of Duties and allowed exceptions
  - Team Manager restrictions (using Approver Lists)
  - Role Owner restrictions (using Approver Lists)
- Security change control (SCC) – Active controls for Security/Menu Promotion or Fix-Merge:
  - SoD Validation activity
  - Test Approval activity
- Security change control (SCC) – Active controls for Role Assignment Promotion:
  - SoD Validation activity
  - Test Approval activity

Assess effectiveness of existing configuration

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.)

ALLOut Control Verifications (VERIFY-C)

Access Change Auditing (Risk Detection) in JD Edwards
(validating installed ALLOut software)

Synopsis:

Assess your JD Edwards system access post-change auditing process

"Get clarity from the specialist JDE security company"

Access Change Auditing (Risk Detection) in JD Edwards

(validating installed ALLOut software on your system)

Key Features

Deliverable: An ALLOut-certified verification of your **post-change (detective)** audit review processes, assessing whether they provide effective oversight of ongoing changes to security access within JD Edwards.

Approach: The audit is conducted using **ALLOut reports, inquiries and configuration views** (via menu program PAOS0001), and the JD Edwards Data Browser only. Your data will not be copied or exported. No changes will be made within your system.

Objective: Provide documentary evidence to satisfy external audit requirements.

Engagement

Two Audit Credits – allocated to:

- One 3-hour session - **with 'take control' access to your system using Teams or Quick Assist**.
  - If there are insufficient permissions, **the audit will be terminated** and a credit note provided.
  - ALLOut software must be pre-installed and the product license active.
  - ALLOut for E1 Version 4.1 is advised.
- Off-screen analysis of collected information to produce your report.

Audit Coverage

Review 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

Review (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

Assess effectiveness of existing configuration