JD Edwards Security Audits

(ALLOut-Certified)

JD Edwards Security Audits (ALLOut-Certified):

CER1A – Change Controls:
User Provisioning (incl. Role Assignment) Controls

CER1B – Change Controls:
JD Edwards System Integrity Controls

CER1C – Change Controls:
JD Edwards Access: Security Controls

CER2A – Compliance:
Information Security Standards (ISO/IEC)

CER2B – Regulatory Compliance:
Regulatory Personal Data Risk (GDPR/CCPA)

CER2C – Regulatory Compliance:
Oracle JD Edwards User Licensing

CER3A – Regulatory System Access:
User SoD Risk Analysis

CER3B – System Access:
User Functional Access by Menu

CER3C – System Access:
User Functional Critical Access

CER3D – System Access:
Role Functional Critical Access with Active User Assignments

CER3E – System Access:
Row Security Access (incl. Company & Business Unit)

Change Controls (CER1A):

User Provisioning Controls

including Role Assignment Controls

Report on your User Provisioning processes and controls:

"Includes user onboarding & offboarding, profile creation & removal, password policies and environment enabling, as well as key role assignment (and therefore access) processes & controls."

Your business requirements are the driver: If your need is for managed services, project resources or otherwise beyond the scope of our service packages, we recommend one of our excellent partners.

Fixed deliverables: We will assess your current risk exposure and provide a comprehensive report of our findings together with best-practice recommendations for going forward.

Change Controls: User Provisioning Controls (including Role Assignment Controls)

Audience:

Team members tasked with internal compliance or preparing for external audit
Team members able to ensure access to the below policies and for verification of controls

Key Considerations and Engagement Length

- **Typical engagement of 2 - 3 days – depending on company size**
- The **deliverable** is an ALLOut-certified report of the assessment of your current situation
  - Requires a subscription to **Risk Management** (with **ProfilePlus** for profile clean-up)
- ALLOut controls not currently in place may be recommended subject to findings
- Access to the client system should be set up by the client before the assessment
- The client does not need to be present for all data sampling activity

Standard Agenda

Discuss Risk Exposure

- Understanding business objectives (i.e., Fraud and Data Integrity)
- Review previous audit findings

Report & Recommendations: Change Control Policies

- User Provisioning
- Unique IDs in use with no generic IDs, Naming convention & User access policy statement
- Profile creation and removal
- Password strength and change frequency
- Role assignment approval process (including update, inquiry & data roles)
- IT admin users
- Redundant profile clean-up

Report & Recommendations: Change Control Sampling

- Executive Summary
- Recommended periodicity of controls review
- Profile updates sampling (PCML0250)
- Profile creation & Password reset
- Role updates sampling (PCML0250)
- Role Creation approval
- Role Environment enabling
- Security Change Controls
- Redundant data clean-up (PDIS0400)
- Redundant profile Clean-up (PCML0930)
  - User update controls
  - Security update controls and Security Change Control
- Role Assignment sampling (PCML0250)
- User provisioning approver controls (and approver lists)
- Request and approval activity
- Restricted role assignment activity
- Role-based SoD Rules change activity

JD Edwards Security Audits

(ALLOut-Certified)

JD Edwards Security Audits
(ALLOut-Certified):

CER1A – Change Controls:
User Provisioning Controls
& Role Assignment Controls

CER1B – Change Controls:
JD Edwards System Integrity Controls

CER1C – Change Controls:
JD Edwards Access Security Controls

CER2A – Compliance:
Information Security Standards
(ISO/IEC)

CER2B – Compliance:
Regulatory Personal Data Risk
(GDPR/CCPA)

CER2C – Compliance:
Oracle JD Edwards User Licensing

CER3A – System Access:
User SoD Risk Analysis

CER3B – System Access:
User Functional Access by Menu

CER3C – System Access:
User Functional Critical Access

CER3D – System Access:
Role Functional Critical Access
& Active User Assignments

CER3E – System Access:
Row Security Access including
Company & Business Unit Access

Change Controls (CER1B):

JD Edwards System Integrity Controls

Report on your System Integrity process controls.

"Includes JDE & ALLOut system change controls, program development change control, computer Operations and UDOs"

Your business requirements are the driver: If your need is for managed services, project resources or otherwise beyond the scope of our service packages, we recommend one of our excellent partners.

Fixed deliverables: We will assess your current risk exposure and provide a comprehensive report of our findings together with best-practice recommendations for going forward.

Change Controls: JD Edwards System Integrity Controls

Audience:

Team members tasked with internal compliance or preparing for external audit
Team members able to ensure access to the below policies and for verification of controls

Key Considerations and Engagement Length

Typical engagement of 2 -3 days – depending on company size

- The deliverable is an ALLOut-certified report of the assessment of your current situation
  - The assessment requires a subscription to Risk Management, with existing configuration of ALLOut auditing an advantage, and to ProfilePlus (for PDIS0400)
- Access to the customer system should be set up by the customer before the assessment
  - The customer does not need to be present for all data sampling activity

Standard Agenda

Discuss Risk Exposure

- Understanding business objectives (i.e., Fraud and Data Integrity)
- Review previous audit findings

Report & Recommendations: Change Control Policies

- JDE and ALLOut system controls
  - System Auditing (F9312) and change logs
  - Physical Server Access
  - External system interface access security
- Program Development Change Control
  - Change management and emergency changes policy
  - Testing, approval & mitigation
  - Version (option update)
  - Redundant objects clean-up
- Computer Operations
  - Batch job scheduling, monitoring & resolution of failed jobs
  - Backup & disaster recovery and incident handling
  - Patch management

Report & Recommendations: Change Control Sampling

- Executive Summary
- Recommended periodicity of controls review
- ALLOut Controls Configuration sampling (PCML0250)
  - UDO Features
  - Password policy

JD Edwards Security Audits
(ALLOut-Certified)

JD Edwards Security Audits (ALLOut-Certified):

CER1A – Change Controls:
User Provisioning Controls
& Role Assignment Controls

CER1B – Change Controls:
JD Edwards System Integrity Controls

CER1C – Change Controls:
JD Edwards Access Security Controls

CER2A – Compliance:
Information Security Standards
(ISO/IEC)

CER2B – Compliance:
Regulatory Personal Data Risk
(GDPR/CCPA)

CER2C – Compliance:
Oracle JD Edwards User Licensing

CER3A – System Access:
User SoD Risk Analysis

CER3B – System Access:
User Functional Access by Menu

CER3C – System Access:
User Functional Critical Access

CER3D – System Access:
Role Functional Critical Access
& Active User Assignments

CER3E – System Access:
Row Security Access including
Company & Business Unit Access

Change Controls (CER1B):

JD Edwards System Integrity Controls

Report on your System Integrity process controls.

"Includes JDE & ALLOut system change controls, program development change control, computer Operations and UDOs"

Your business requirements are the driver: **If your need is for managed services, project resources or otherwise beyond the scope of our service packages, we recommend one of our excellent partners.**

Fixed deliverables: We will assess your current risk exposure and provide a comprehensive report of our findings together with best-practice recommendations for going forward.

Change Controls: JD Edwards System Integrity Controls

Audience:

Team members tasked with internal compliance or preparing for external audit

Team members able to ensure access to the below policies and for verification of controls

Key Considerations and Engagement Length

Typical engagement of 2 -3 days – depending on company size

- The deliverable is an ALLOut-certified report of the assessment of your current situation
  - The assessment requires a subscription to Risk Management, with existing configuration of ALLOut auditing an advantage, and to ProfilePlus (for PDIS0400)
- Access to the customer system should be set up by the customer before the assessment
  - The customer does not need to be present for all data sampling activity

Standard Agenda

Discuss Risk Exposure

- Understanding business objectives (i.e., Fraud and Data Integrity)
- Review previous audit findings

Report & Recommendations: Change Control Policies

- JDE and ALLOut system controls
  - System Auditing (F9312) and change logs
  - Physical Server Access
  - External system interface access security
- Program Development Change Control
  - Change management and emergency changes policy
  - Testing, approval & mitigation
  - Version (option update)
  - Redundant objects clean-up
- Computer Operations
  - Batch job scheduling, monitoring & resolution of failed jobs
  - Backup & disaster recovery and incident handling
  - Patch management

Report & Recommendations: Change Control Sampling

- Executive Summary
- Recommended periodicity of controls review
- ALLOut Controls Configuration sampling (PCML0250)
  - UDO Features
  - Password policy