JD Edwards Security Audits

(ALLOut-Certified)

Regulatory Compliance (CER2A):

Information Security Standards

(e.g., ISO/IEC)

Verify steps taken to comply with JDE Information Security Management System (ISMS) industry standards (ISO, IEC, etc.).

Report on your policies around system access, change management and system monitoring.

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

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

CER2C – Regulatory 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

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.

Regulatory Compliance: Information Security Standards (ISO/IEC)

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 2-4 days – depending on company size

- The deliverable is an ALLOut-certified report of the assessment of your current situation
  - Access to the customer system should be set up by the customer before the assessment
- The customer will need to be present for all activity other than production of the final report

Standard Agenda

Discuss Risk Exposure

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

Report & Recommendations: Access Control Policies

  - Executive Summary
  - Recommended periodicity of review
- Employment Security Controls
  - On-Boarding
  - Employment contracts & responsibilities
  - Ongoing education & training
  - Off-Boarding: Asset & access removal
- Access to privileged accounts
  - Access to developer software (e.g., OMW)
  - Access to IT (Administrator) accounts
  - Administrator access to production data
  - Management approval process
- Rules for system access (for users and roles)
  - Password policy
  - Periodic review & approval
  - Business owner control of access to applications & data
  - Environment access
  - Update, Inquiry & Data role assignment
- Removal of redundant data
  - Inactive and leaver account disabling
  - Access & security records clean-up
  - Redundant profile exposure
  - IT profile exposure

Report & Recommendations: Operational Control Policies

- Change management control, testing & promotion
  - Security incident management process (including escalation policy)
- System monitoring
  - Audit logging & retention

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

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

CER2C – Regulatory 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

Regulatory Compliance (CER2B):

Regulatory Personal Data Risk
(e.g., GDPR/CCPA)

Verify the steps taken to comply with regulatory data protection requirements (GDPR, CCPA, etc.).

Includes identifying key JDE personal data and personal data protection & incident handling policies; designing & documenting database security and system access procedures.

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.

Regulatory Compliance: Personal Data Risk (GDPR/CCPA)

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
- 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., best-practice and regulatory)
  - Review previous audit findings
- Identify and document personal data in JD Edwards
  - HR data (e.g., F060116)
  - Address book (e.g., F0111)
  - Media object attachments (i.e., F00165)

Report & Recommendations: System Access Policies

- Executive Summary
- Recommended periodicity of review
- Internal data confidentiality policies
  - Review Incident handling & escalation procedure
  - Review staff training procedures
- User Lifecycle: Creation (and approval), access modification and termination
  - Terms of usage training: Computer locking and password protection
  - Limited administrator and programmer accounts
  - Limited access to data browser
- Database security
  - Controlled access to interfacing systems
  - Personal data removed from sandpit and developer systems
  - Redundant profiles retention/removal
  - Best-practice password policy
- Business user access to programs within application
  - Role-based deny-all and grant-back access
  - Limiting Read-only access with Menu Filtering & E1 Pages

Report & Recommendations: Data Access Controls Sampling

- Effective database-level security
- Media Object security – for images and contracts
- Address Book Data Privacy – for telephone numbers, email, and physical addresses
- Row Security – for sensitive data in relevant tables (e.g., within HR module)
- Data masking and/or Column security

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

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

CER2C – Regulatory 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

Regulatory Compliance (CER2C):

Oracle JD Edwards User Licensing

Verify the steps taken to comply with Oracle JDE User Licensing exposure; including user counts and module usage.

We recommend to you how to implement proactive user identification and cleanup procedures based on actual or potential access.

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.**

Regulatory Compliance: Oracle JD Edwards User Licensing

Audience:

Team members tasked with internal compliance or preparing for external audit
Team members able to discuss the Oracle licensing policy at their company

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 Reporting (for PCML0600) with SoDMaster an advantage, or ProfilePlus (for PDIS0400) depending on the approach taken
- Access to the customer system should be set up by the customer before the assessment
  - The customer does not need to be present after initial meetings

Standard Agenda

Determine Methodology

- Understanding business objectives
  - Review previous license audit findings
  - Review modules in use (note P99410 shows additional features)
- Review licensing alternative methodologies and their availability
  - Actual (past) program access – using 9.2 Object tracking (not provided using this Audit)
  - Potential program access –using SoDMaster critical list and applied security (PCML0600)
  - Actual (past) data updates – using System Usage Inquiry (PDIS0400)
- Establish Parameters to use
  - Review business specific criteria (e.g., module availability)
  - Time periods for past access
  - Module identification (e.g., JDE product code)

User Identification and Pre-Audit Clean-up

- Identify all inactive and non-production users (PCML0960)
- Remove redundant user profiles (PDIS0300)
- Document redundant user identification & removal procedure

Report: System usage

- Executive Summary
  - Recommended periodicity of review
- Report
  - Group user profiles for easier reporting
  - Report modules used by profile
  - Identification of module usage