ALLOut Security

Security Audits

Security Audits Catalog

Version 1.0.1

Updated September 2023

ORACLE Validated Integration

JD Edwards EnterpriseOne

Security Audits Catalog

ALLOut Audits Catalog

Summary

Audits - to report on your existing security and controls

- ✓ **JD Edwards E1 Security Audit (ALLOut-Certified)**

FAQs:

Who can request an audit?
Audits are available to any JD Edwards user.

Can audits be customized or extended?
Our audits come with a standard agenda for delivery in blocks of half-days (3 hours approx.).
If you require assistance beyond our specialist offering, we are proud to recommend further support from our extensive partner network of specialist service-providers.

Does there need to be a signed agreement?
Yes, we use a "Statement of Work" document to ensure we follow a clearly defined agenda.

What is the next step?
If after looking at this document, you believe an audit can help you, log on to our Customer Portal and contact the Customer Success team.
Once the agreement is signed, the session(s) can be scheduled using our website to book from available timeslots.
We endeavor to provide suitable timeslots for America and EMEA time zones.

Can ALLOut provide IT services in addition to those advertised on the website?
No, our business is software development – we offer pre-defined workshops and security audits - at a subsidized cost, not 'hourly-rate' or similar services.
Our aim is to help you take ownership of your system rather than be a service-provider.

All audits come with an agreed agenda - the exact length of the audit will be specified within.

ALLOut is a software house: These audits are designed to the meet specific objectives outlined only.

If additional assistance is required, we will recommend one of our specialist service-provider partners.

JD Edwards E1 Security Audit (ALLOut–Certified)

- ✓ Prepare for external audit and improve compliance with an ALLOut audit.
- ✓ A certified report will typically include best-practice recommendations to ensure effective, demonstrable progress to management and auditors.
- ✓ Client engagement is limited to providing the required access to the system.

1. Change Control Audits – Choose from listed agendas (2-3 Days):

CER1A User Provisioning (including Role Assignment) Controls

Description

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.

CER1B JD Edwards System Integrity Controls

Description

Report on your System Integrity processes & controls.
Includes JDE & ALLOut system change controls, program development change control, computer operations and use of UDOs.

CER1C JD Edwards Access: Security Controls

Description

Report on your System Access processes & controls.
Includes best practices on security updates and the ALLOut change controls designed to manage access changes resulting from security updates and manage segregation of duties risk.

2. Regulatory Compliance Audits – Choose an agenda option (2-4 Days):

CER2A Information Security Standards (ISO/IEC)

Description

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.

CER2B Regulatory Personal Data Risk (GDPR/CCPA)

Description

Verify steps taken to comply with regulatory data protection requirements (GDPR, CCPA, etc.).
Includes identifying key JDE personal data, personal data protection & incident handling policies, designing & documenting database security and system access procedures.

CER2C Oracle JD Edwards User Licensing

Description

Verify steps taken to comply with Oracle JDE User Licensing; including user count & module use.
Includes recommendations on implementing proactive user identification and cleanup procedures based on actual or potential access.

3. System Access Audits – Choose an agenda option (2-4 Days):

CER3A User SoD Risk Analysis

Description

Report on JDE system's current exposure to Segregation of Duties.
Includes recommendations on effective, documented SoD rules and processes, as well as remediation or mitigation strategies to improve security and manage reporting.

CER3B User Functional Access by Menu

Description

Report on users' current access to your JDE system, considering menu design and security permissions.
Includes recommendations on effective security controls designed to limit system access based on "least privilege" role access and documented rules.

CER3C User Functional Critical Access

Description

Report on users' current access to your JDE system considering program-level security permissions only.
Includes recommendations on effective security controls designed to limit system access based on "least privilege" role access and documented rules.

CER3D Role Functional Critical Access with Active User Assignments

Description

Report on current access to the functionality of your JDE system by analyzing the program-level security permissions at role level and the assignment of those roles to your users.
Includes recommendations on effective security controls designed to limit system access based on "least privilege" role access and documented rules.

CER3E Row Security Access (including Company & Business Unit)

Description

Report on current access to your JDE system considering your JDE Row security permissions only.
Includes recommendations on effective security controls designed to limit access to the data of companies or business units.