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

System Access (CER3A):

User SoD Risk Analysis

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."

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.

System Access: User SoD Risk Analysis

Audience:

Team members tasked with internal compliance or preparing for external audit
Team members able to confirm the key SoD risks of their organization

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
  - The assessment requires a subscription to Risk Reporting with SoDMaster an advantage
- 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

Discuss Risk Exposure

- Review current security set-up:
  - Understanding objectives when separating responsibilities (i.e., Fraud and Data Integrity)
  - Review previous audit findings if any
  - Understand systems in use (i.e., if beyond JD Edwards)
  - Review any previous SoD remediation & mitigation efforts
- Review Security model in use
  - Multiple Roles & the Role Chooser
  - Deny All vs Menu Filtering Security
  - User-level security exceptions
  - *Public Access
  - Action Code vs Application Security: Read-Only vs Update permissions

Recommendations

- Security best practices
  - Removing User-level security exceptions
  - Implementing Deny All
  - Disabling Role Chooser (and resolving any resulting multiple role sequencer issues)
- System Access best practices
  - SoD remediation & mitigation
  - User access review and & approval
  - Security access change control
  - Role assignment approval

Report

  - Executive Summary
  - Recommended periodicity of review
- Current SoD Rule Set in Use (PCML0260)
  - Lists of critical programs
  - Best practices
- User SoD Reporting (PCML0600)
  - Within-Role SoD exposure
  - Redundant and IT profile exposure

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

System Access (CER3B):

User Functional Access by Menu

Report on users' current access to your JDE system, considering menu designs and security permissions:

"Includes recommendations on effective security controls designed to limit system access based on "least privilege" role access and documented rules."

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.

System Access: User Functional Access by Menu

Audience:

Team members tasked with internal compliance or preparing for external audit
Team members able to confirm the menus in use at their company

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
  - The assessment requires a subscription to MenuPlus with SoDMaster an advantage
- 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 Risk Exposure

- Review current security set-up
  - Understanding business objectives (i.e., program controls vs menu controls)
  - Review previous audit findings if any
  - Understand systems in use (i.e., if beyond JD Edwards)
  - Review menu design: Task Views and Favorites vs E1 Pages
- Review Security model in use
  - Multiple Roles & the Role Chooser
  - Deny All vs Menu Filtering Security
  - User-level security exceptions
  - *Public Access
  - Action Code vs Application Security: Read-Only vs Update permissions
  - Effects of Row Security on functional access

Recommendations

- Security best practices
  - Removing User-level security exceptions
  - Implementing Deny All
  - Moving to (SoD-free) role-based access model
  - Disabling Role Chooser (and resolving any resulting multiple role sequencer issues)
- Process best practices
  - Security access change control
  - Role assignment approval
  - User provisioning and access rights

Report

  - Executive Summary
  - Recommended periodicity of review
- User Access Reporting (PCML0725)
  - Current Menus in Use: Effects of Menu Filtering
  - Application and Action Security
  - Functional security loopholes (e.g., Exits and FastPath)
  - Redundant and IT profile exposure

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

System Access (CER3C):

User Functional Critical Access

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."

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.

System Access: User Functional Critical Access

Audience:

Team members tasked with internal compliance or preparing for external audit
Team members able to confirm the critical processes of their organization

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 with SoDMaster an advantage
- 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

Discuss Risk Exposure

- Review current security set-up
  - Confirm what are critical business processes
  - Review previous audit findings if any
  - Understand systems in use (i.e., if beyond JD Edwards)
- Review Security model in use
  - Multiple Roles & the Role Chooser
  - Deny All
  - User-level security exceptions
  - *Public Access
  - Action Code vs Application Security: Read-Only vs Update permissions
  - Effects of Row Security will not be considered to determine functional access

Recommendations

- Security best practices
  - Removing User-level security exceptions
  - Implementing Deny All
  - Disabling Role Chooser (and resolving any resulting multiple role sequencer issues)
  - Moving to (SoD-free) role-based access model
- System access best practices
  - Security access change control
  - Role assignment approval
  - User provisioning and access rights

Report

  - Executive Summary
  - Recommended periodicity of review
- User Access Reporting (PCML0600)
  - Application and Action Security
  - Functional security loopholes (e.g., Exits &FastPath)

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

System Access (CER3D):

Role Functional Critical Access & Active User Assignments

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."

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.

System Access: Role Functional Critical Access & Active User Assignments

Audience:

Team members tasked with internal compliance or preparing for external audit
Team members able to confirm the critical processes of their organization

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
  - Requires a subscription to Risk Reporting and ProfilePlus with SoDMaster an advantage
- 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

Discuss **Risk Exposure**

- Review current security set-up
  - Understanding business objectives (i.e., critical business processes)
  - Review previous audit findings if any
  - Understand systems in use (i.e., if beyond JD Edwards)
- Review Security model in use
  - Multiple Roles & the Role Chooser
  - Deny All
  - User-level security exceptions (should not be present)
  - *Public Access
  - Action Code vs Application Security: Read-Only vs Update permissions
  - Effects of Row Security and user-level exceptions on functional role access

Recommendations

- Security best practices
  - Removing User-level security exceptions
  - Implementing Deny All
  - Moving to (SoD-free) role-based access model
  - Disabling Role Chooser (and resolving any resulting multiple role sequencer issues)
- System Access best practices
  - User provisioning and access rights
  - Security access change control
  - Role assignment approval

Report

  - Executive Summary
  - Recommended periodicity of review
- Role Access Reporting (PCML0600)
  - Application and Action Security
  - Functional security loopholes (e.g., Open system & FastPath)
- Role Assignment Reporting (PCML0960)
  - Redundant profile exposure
  - IT profile exposure

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

System Access (CER3E):

Row Security Access
including Company & Business Unit Security

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."

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.

System Access: Row Security Access

including Company & Business Unit Security

Audience:

Team members tasked with internal compliance or preparing for external audit
Team members able to confirm the security business objectives at their company

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
  - The assessment is predicated on subscription to Risk Reporting with CombiRoles a requirement for use of PMUR0100
- 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

Discuss Risk Exposure

- Review current security set-up
  - Understanding business objectives when securing data (e.g., separating legal entities)
  - Review previous audit findings if any
  - Data items and Tables currently secured
- Review Security model in use
  - Multiple Roles & the Role Chooser
  - Inclusive Vs Exclusive Row Security
  - User-level security exceptions
  - *ALL file “Deny All” vs specific tables

Recommendations

- Security best practices
  - Data items missing
  - User-level security exceptions
  - *ALL files vs specific tables
  - Forcing Multiple Roles & Sequencer Issues
  - Implementing Inclusive Row Security
- Process best practices
  - Security change control
  - Role assignment approval
  - User provisioning and access rights

Report

  - Executive Summary
  - Recommended periodicity of review
- Current Access Reporting: Role and User Access (PCML0650)
  - Companies
  - Business Units
- Current Access Reporting: Role and User Access (PMUR0100)
  - Address Book and other data types