

Level 1 Assessment: Oracle E-Business Suite GRC Health Check

Overview:

This Level I Assessment covers a broad array of best practices noted in the book Oracle E-Business Suite Controls: Application Security Best Practices written by Jeffrey T. Hare, CPA CISA CIA. This assessment offers a 10,000' view of your organization's compliance with various application security best practices. The assessment will give you a great 'first look' at your organization's application security environment. The assessment includes analysis, interaction and expertise from one of the industry's top experts, Jeffrey Hare.

The Assessment Includes:

An assessment of critical controls related to application security from a series of eight SQL statements. In those, we will address:

1. Upgrade risk – identify risks your organization can expect when patching, applying family packs, and upgrading from 11i to R12
2. Users with access to AZN menus and related risks (at top level menu only)
3. Identification of seeded users – recommendations on which ones to disable and monitoring strategies for those that need to remain active
4. Best practices for generic users, such as job scheduling users – review current security design and develop monitoring strategies
5. Identification of privileged users and strategies for minimizing their access – high level recommendations (detailed analysis and recommendations can be provided in Level II assessment related to privileged users)
6. User password policy compliance for application-level users(not database accounts)
7. Review critical security and controls-related profile options (Password-related, Utilities: Diagnostics, Failed Attempts, SignOn Audit) at all levels
8. Users with access to high risk responsibilities
9. Stale users
10. Users that are possibly terminated based on their HR record
11. Users with no employee record assigned
12. Employees with more than one user record assigned

Not included:

Function level analysis of Segregation of Duty conflicts, high risk functions, and access to sensitive data. This can be provided via a Level II assessment as a Software as a Service assessment.

**Key Activities:**

1. Client to run the provided extract script to extract key FND data and forward to ERP Risk Advisors
2. ERP Risk Advisors will load of the results from extract scripts into CaoSys' CS*Comply XE software for analysis.
3. Results of the analysis, including found issues, will be documented in the assessment report.
4. The results of the assessment will be presented on-line to the client.

Deliverables:

1. Written report of findings and recommendations

Duration:

Approximately one week

References:

“Jeff provided an excellent overview of the existing risks within our Oracle EBS, and detailed recommendations to mitigate them. The assessment identified numerous risks relating to both fraud, SoD conflicts and non compliance with local policies. The SQL queries produced a lot of informative data which was later talked through in an easy to understand discussion to get to the core risks and security holes that need to be addressed. The Level 1 Assessment would be an essential starting point for Auditors, Oracle DBA’s and Central IT teams in companies where the Oracle EBS is used as a core System.” – IT Auditor, local government

“I recommend any organization to take advantage of Jeff’s Level 1 logical access assessment for Oracle EBS. Our IT organization was able to prioritize the clean-up of SOD conflicts with an easy game plan to follow. This was especially helpful to me as an auditor because our company just acquired another company that uses Oracle EBS. Jeff continues to advance Oracle EBS tools that are user-friendly and make a big impact!” – IT Auditor, Telecommunication Manufacturer

ERP Risk Advisors is a leading provider of Risk Advisory services for organizations using Oracle Applications. We provide [consulting](#) and [training](#) services related to compliance, security, risk management, and controls. We also assist organizations in implementing GRC-related software from industry-leading companies such as Oracle, Absolute Technologies, CaoSys, ConfigSnapshot, Greenlight Technologies, and MentiSoftware. Contact us at info@erpra.net or 970-324-1450.