

See the rocks.

Assessing your Oracle E-Business suite controls



Organisations implement Enterprise Resource Planning (ERP) systems like Oracle E-Business suite (Oracle) to improve and automate business processes. Expected benefits of implementation include a reduction in the cost of operations, greater asset efficiency and enhanced quality of information. Oracle can help you achieve this, however in our experience there is one area that proves to be difficult to get right.....controls.

The Oracle Controls challenge

From our experience, organisations with Oracle struggle to gain an understanding or visibility of their Oracle controls, especially due to the limited out-of-the-box security/controls reports. This lack of visibility can include:

- **Access to sensitive functions.** Organisations are unable to identify who within their business has access to sensitive Oracle functions, such as amending supplier bank accounts or updating configuration items

“Organisation’s struggle to gain visibility of Oracle controls, as a result they are unaware of the associated risk exposure.”

- **Segregation of duties.** Due to the complexity of the Oracle Access Controls model, organisations struggle to report on whether they are breaching segregation of duties
- **Business process controls.** The organisation is unsure whether their business processes are utilising appropriate Oracle system and configuration controls
- **Database security controls.** The controls at the infrastructure layer are rarely considered and therefore it is unknown whether the database and infrastructure underpinning Oracle is secure
- **Limited audits.** Typically auditors only conduct limited tests around general computer control areas (such as password controls).

As a result, few organisations with Oracle have a real understanding of the status of their Oracle controls or the extent of their associated risk exposure.

The implications of poor Oracle controls visibility

Sensitive data

Oracle can store sensitive data such as customer, supplier and HR information, which is needed to automate key business processes. Where Oracle is inappropriately

controlled, the risks to your business can range from data leakage of sensitive details, purchase to pay fraud and material misstatements of accounts.

Compliance requirements

There is an increasing requirement from compliance stakeholders to report on and demonstrate effectiveness of key Oracle controls. Where the controls implemented are manual or resource intensive, they can result in an unnecessary overhead and the business complaining about the “controls burden”.

Reputation

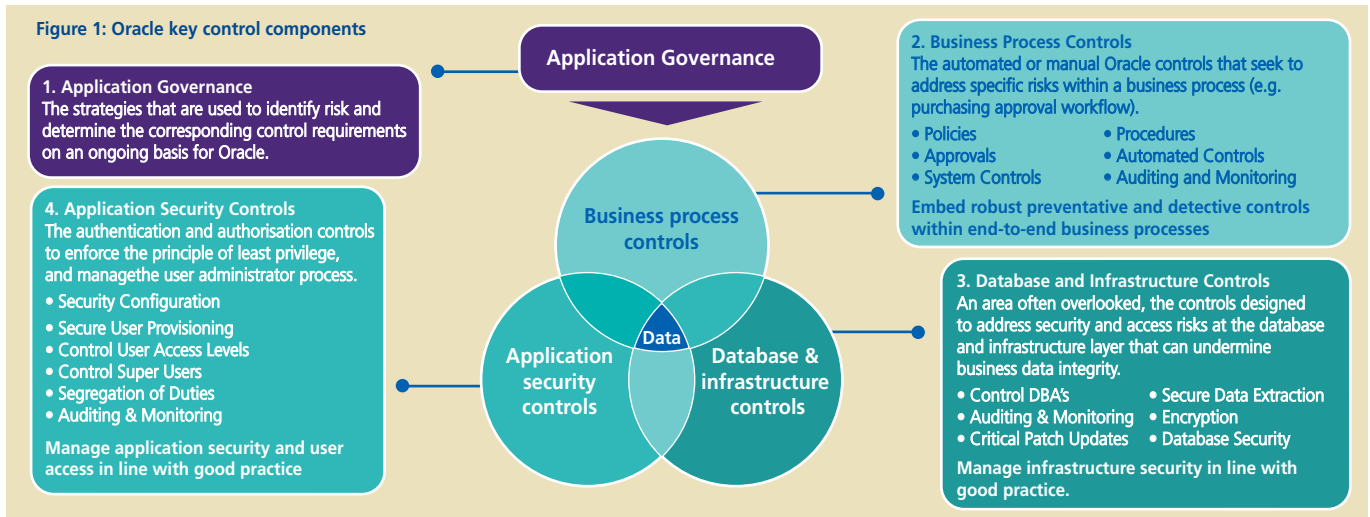
Organisations seek a competitive advantage through transforming their internal business practices, such as shared service centres and outsourced functions, which can significantly impact your Oracle system. Maintaining a good reputation internally and externally in the market place is key. Public control failures can result in irrevocable damage to your brand, sales and even shareholder value.

Our approach to Oracle Controls

We have a proven approach to assessing Oracle controls which is supported by our proprietary Oracle Application Security Integrity Suite (OASIS) and which is based on practical experience having being deployed as part of Oracle implementations.

See the rocks

Assessing your Oracle E-Business suite controls



It is easy to underestimate the complexity and inter-relationships between the Oracle controls components as illustrated in Figure 1. Our approach therefore includes an assessment of controls in each of the four Oracle control components. Typically, an assessment would include the following stages:

- Understand the organisation's governance structure, risk and controls framework, and supporting policies / procedures in relation to the Oracle environment
- Use OASIS to provide information on the organisation's Oracle business process controls, Oracle application security, Oracle segregation of duties, access to sensitive Oracle functions and Oracle database security
- Run workshops with key members in the organisation to assess controls within the four Oracle control components and discuss / validate the findings from OASIS
- Provide a report including our findings and a roadmap outlining potential remedial activities and recommendations to further improve, optimise and automate Oracle controls.

This final report will be in a non-technical language and will be supported by Oracle technical details in the appendices. This will allow the business to understand the risks, and the technical community to understand what may need to be changed from a systems perspective.

As a result, through increased visibility and understanding of your Oracle controls, an organisation is able to take the first step in gaining control.

Our Oracle control services

In addition to our Controls assessment capabilities (as referred to in this document), the Deloitte Oracle Controls team can also help implement and optimise your Oracle controls.

- **Controls implementation**
Help you get controls right from the start by working as part of an Oracle implementation programme to design and embed controls within the initial solution
- **Controls optimisation**
We can optimise your Oracle controls through automation and rationalisation to streamline existing controls or implement automated control solutions.

The Deloitte Difference

- Deloitte is a leader in Enterprise Risk Services. Our dedicated Oracle Controls team has unrivalled knowledge and experience having assessed, designed and transformed controls on more than 100 Oracle implementations
- Unique skill set. Our dedicated team members have the unique combination of deep technical Oracle skills and a background in risk and controls, allowing us to engage effectively with an organisation's compliance, business and IT functions. We therefore understand your control requirements, and how effectively to implement these from an Oracle perspective
- Implementation capabilities. Our team can implement the solution for Oracle controls, not just assess. This is supported by our Partner relationship with Oracle
- Supporting Toolsets. Deloitte has developed bespoke toolsets (OASIS) to enable us to validate Oracle application security, database and business process controls.

Contacts

Andy Morris
 Email: admorris@deloitte.co.uk
 Phone: +44 (0)20 7007 3308

Or visit us at
www.deloitte.co.uk/oraclecontrols

In this publication, Deloitte refers to one or more of Deloitte Touche Tohmatsu ('DTT'), a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither DTT nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the DTT Verein.

In the UK, Deloitte & Touche LLP is the member firm of DTT, and services are provided by Deloitte & Touche LLP and its subsidiaries. For more information, please visit the firm's website at www.deloitte.co.uk

Deloitte & Touche LLP is authorised and regulated by the Financial Services Authority.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication.

Deloitte & Touche LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte & Touche LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© Deloitte & Touche LLP 2008. All rights reserved.

Deloitte & Touche LLP is a limited liability partnership registered in England and Wales with registered number OC303675. A list of members' names is available for inspection at Stonecutter Court, 1 Stonecutter Street, London EC4A 4TR, United Kingdom, the firm's principal place of business and registered office. Tel: +44 (0) 20 7936 3000. Fax: +44 (0) 20 7583 1198.