Just How Secure Is Your ERP System?

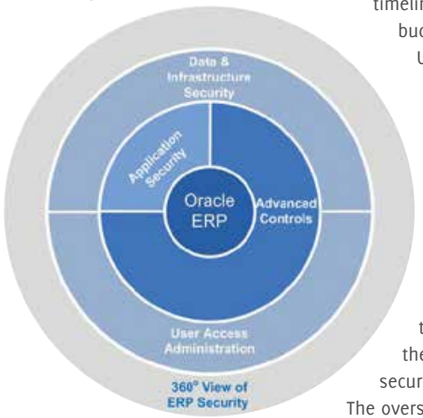
KPMG assists companies in protecting their most valuable data and assets.

KPMG LLP, the audit, tax, and advisory firm, has a long history of providing companies with a depth of expertise in an array of areas including risk and security assessment and management. As an Oracle Platinum Partner, KPMG focuses on reducing risk for companies implementing or managing large enterprise resource planning (ERP) systems that underpin their financial accounting and operational processes. Laeeq Ahmed, managing director at KPMG, discusses KPMG's "Securing the ERP" approach and what it can do for companies running Oracle ERP solutions.

What are some common mistakes made in implementing an ERP security strategy?

Traditionally, ERP project teams are all too consumed with enabling core ERP functionality, prioritizing implementation tasks and activities to align with timeline limitations and budget constraints. Unfortunately, all too often, this strategy means that security concerns are lost in the shuffle, and only after the ERP system is up and running does the team appreciate the serious gaps in security and controls. The oversights and compromises that are made during implementation wind up leading to remediation projects post-go-live to make necessary corrections. These remediation projects are typically very disruptive, extremely expensive, and time-consuming.

KPMG Securing the ERP



What are the risks facing organizations that don't have secure ERP systems?

Generally speaking, there are three types of risks that organizations face in terms of their ERP system. The first is unauthorized access. ERP systems typically come with a set of standard roles that are assigned to users based on what functional task they are responsible for within the organization, but there's always the risk that users could make unauthorized updates, create fraudulent transactions, or submit an entry with preventable transaction errors. The second is noncompliance with regulatory or security requirements. The third is reporting—too often, the inherent reporting capabilities of ERP systems don't meet users' specific needs, and then they resort to other tools such as Microsoft Excel or Microsoft Access, which of course have their security challenges. Obviously, the stakes are enormous when it comes to vulnerable ERP solutions. Weak ERP security can ultimately lead to not just operational bottlenecks, but fraud, loss of assets, misstatement of financial results, and data privacy compromises.

Why is ERP security complicated?

It's a matter of the sheer number of functional and technical components that have to be taken into account when defining an ERP security and controls program. Bundling user management, internal controls, financial data management and reporting, compliance, and protection against internal and external cyber threats associated with a global user community into an integrated solution is a tall order.

What is KPMG's "Securing the ERP" strategy?

KPMG's Securing the ERP is a 360-degree approach to ERP security and controls, designed to empower businesses to balance the needs of ERP end users with the need to protect sensitive data and transactions. The overall objective of Securing the ERP is to manage the material risks associated with ERP systems by identifying the risks and devising and implementing strategies to protect information confidentiality, integrity, and accessibility. KPMG's approach is acutely focused on minimizing risks, by proactively focusing on security and controls during implementations to prevent costly rework after a new or upgraded ERP solution is operational.

What are the key components of KPMG's approach?

We look at ERP security from a number of different perspectives. Naturally there's application security, which is focused on enabling users and protecting sensitive transactions and data using core ERP application security functionality. We also offer advanced automated controls solutions that are configurable specifically for our client's Oracle ERP systems that provide for preventive and detective transaction controls.

In terms of data and infrastructure, KPMG's strategy focuses on servers, databases, and networks—specifically on guarding against risks such as corruption of backup processes and deletion of data in the database that can bring a poorly executed ERP project, and an entire company, to its knees.

The KPMG 360-degree strategy also zeroes in on the operational aspect of managing ERP users, which can be underappreciated. Organizations need to continually adjust their user access designs to keep up with the ever-changing organizational landscape. In a healthy business, change is the norm, and KPMG's solution helps proactively administer user access in a cost effective manner.

Why has KPMG chosen to partner with Oracle in the ERP security space?

We turned to Oracle solutions in our Securing the ERP strategy because they are tightly integrated and perform seamlessly with Oracle ERP systems. In our engagements, we use Oracle solutions such as Oracle E-Business Suite, PeopleSoft applications, Oracle Audit Vault, Oracle Database Vault, Oracle Advanced Controls, Oracle Access Manager, Oracle Enterprise Single Sign-On, Oracle Identity Manager, Oracle Identity Analytics, and Oracle Directory Services to lock down our clients' ERP security. The breadth of Oracle's product offerings gives us the ability to provide a structured approach to strategically protect our clients' Oracle ERP systems.

How does KPMG add value to Oracle ERP solutions?

KPMG brings a depth and breadth of security and controls expertise to today's ERP security challenges. KPMG's ERP resources know the business advantages of a well-managed ERP system, and they know how to implement the right technology in a given context to not just foster a company's growth and efficiency, but help ensure that its assets and data are protected. As headlines across the globe illustrate every day, security is no longer a "nice to have" option, but rather an imperative that needs to underpin any ERP implementation.

Laeeq Ahmed, Managing Director, KPMG

The KPMG "Securing the ERP" Strategy

The KPMG Securing the ERP strategy is a fit for any company already running Oracle solutions, including Oracle E-Business Suite or PeopleSoft financial applications, as well as for companies considering adding new controls to an existing system or a fresh enterprise resource planning (ERP) installation.

Standard, out-of-the-box Oracle ERP systems have robust functionality to support a wide range of business requirements, including financial reporting, that are "must-haves" for virtually every organization and industry, but often organizations don't activate built-in features, nor do they take full advantage of Oracle Advanced Controls solutions that can be configured to serve their particular needs. KPMG has the expertise to drive that level of customization and mitigate the many risks that can compromise an ERP system, primarily by enabling organizations to support an integrated and holistic controlled and compliant environment.

When it comes to ERP systems, KPMG's IT Advisory Services drill down into application security, advanced controls, data and infrastructure security, and user access administration. KPMG also deploys a risk-based approach that unfolds in five phases: plan, design, build, implement, and monitor.

KPMG's Securing the ERP services are anchored in a deep understanding of the risks, industry nuances, ERP business processes and technologies, and regulatory issues affecting the internal controls environment of companies across industries.

For more information, visit **www.kpmg.com**

KPMG