Maximizing the ERP INVESTMENT

Organizations have, or will invest, a lot of time, effort, and monetary resources in their Enterprise Resource Planning (ERP) initiatives. Many times, the real or even perceived value of the investment is not realized for many years. A factor contributing to this delay is the inability to leverage more than core ERP functionality. The organization had not managed the project effectively enough to get past core features.

Today, ERP project teams still primarily focus on core ERP functionality, prioritizing implementation activities to align with timeline limitations and budget constraints. This tactical approach commonly results in risk and control compromises not fully appreciated, until after go-live. Delayed benefits include reducing IT costs through Identity Management and addressing financial reporting compliance requirements. Once the ERP solution is live and operational, organizations begin to realize the significance of their oversights and compromises and are forced initiate post go-live remediation projects to make the necessary corrections. These projects are disruptive, exponentially more expensive, and time consuming.

Organizations demand more from their ERP investments. A successful ERP project will indeed help streamline processes and reduce the overall cost of doing business. Even though ERPs offers a lot of potential value, they often require enhancements to fully meet management's objectives. These objectives include:

- Reducing Operational Risk
- Increasing Process Effectiveness and Efficiency
- Improving the Bottom Line

Securing the ERP

To help organizations achieve these objectives, KPMG's network of firms has developed its approach to security and controls around the ERP – Securing the ERP. KPMG's Securing the ERP approach is a 360 degree view of ERP security and controls, and is positioned to help industry leading organizations effectively balance the divergent tasks of empowering ERP business users while simultaneously protecting sensitive data and transactions.

Securing the ERP addresses four major quadrants of security and controls:

1 Advanced Controls
2 Application Security
3 Data & Infrastructure
4 User Access Administration

Quadrant: Advanced Controls

Advanced Controls focuses on aligning application controls to business processes. These application controls include native, out-of-the-box ERP controls. They also include additional features that augment existing controls or provide new ones that are not currently available in the application.

Advanced Controls: Key Business Drivers

Quite often, the value realized from an ERP investment does not meet management's expectations until additional features beyond core business processes are enabled. These additional features typically address areas such as:

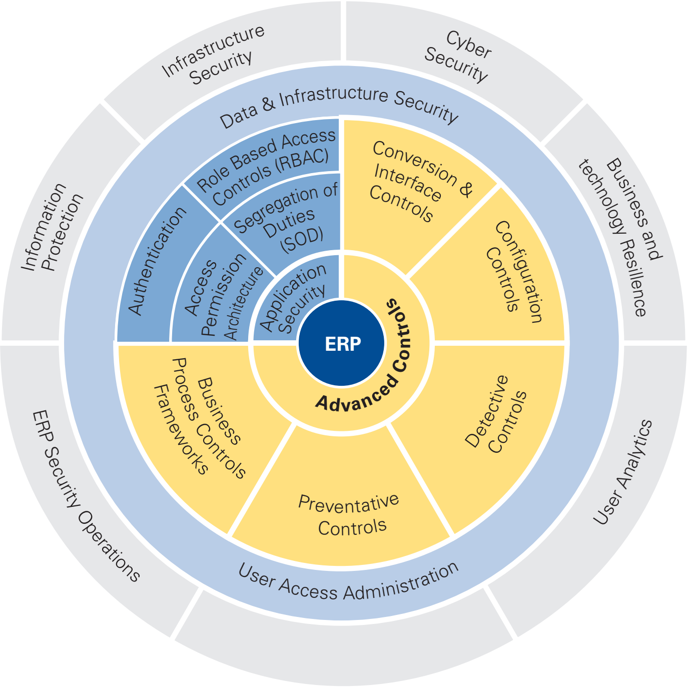
- Improvement for complex and inefficient ERP-centric processes
- lost revenue
- cash leakage
- high configuration and maintenance costs
- greater transparency over sensitive transactions
- reducing the risk for fraud and error

In an ERP implementation, application features and controls addressing many of these items end up on a deferred items list for completion in a subsequent project after go-live.

Advanced Controls: Focus and Scope

Advanced Controls focuses on enabling the application to effectively and efficiently support management's business processes and documented controls. This objective includes the following activities:

- updating the organization's business process controls framework to organize manual controls, ERP application controls and automated controls
- transitioning manual tasks where possible to automated ones


Infrastructure Security
Cyber Security
Business and technology Resilience
User Analytics
ERP Security Operations
Information Protection
Data & Infrastructure Security
User Access Administration
Role Based Access Controls (RBAC)
Segregation of Duties (SOD)
Authentication
Access Permission Architecture
Application Security
Conversion & Interface Controls
Configuration Controls
Detective Controls
Preventative Controls
Business Process Controls Frameworks
ERP
Advanced Controls

Source: GRC Today, October 2015, KPMG International

- leveraging up-front, automated and preventive controls to mitigate process risks
- leveraging automated detective controls to monitor sensitive transactions and data changes
- improving configuration management by tracking and monitoring configuration and master data changes and comparing them to baseline documentation for the ERP instances
- implementing and maintaining effective and efficient conversion & interface Controls
- analyzing, reporting, and remediation user-provisioned segregation of duties issues

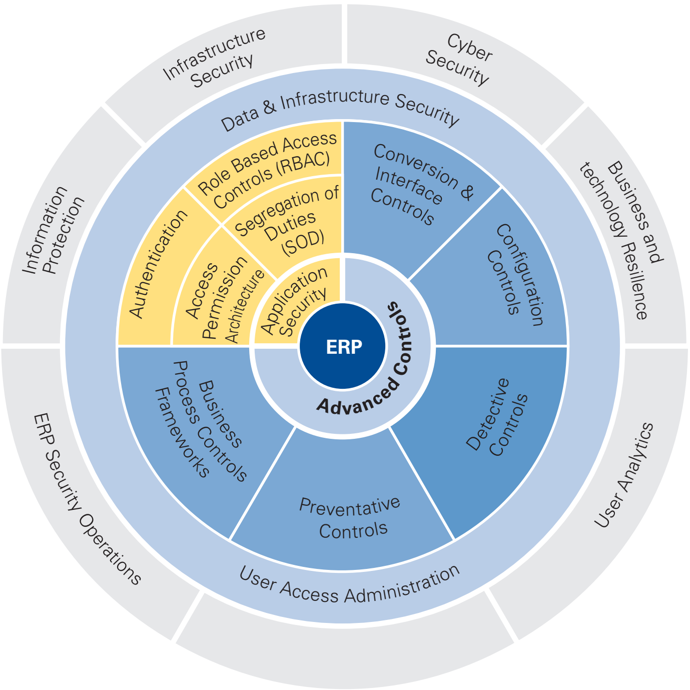
Advanced Controls: Realized Value

The realized value for managing the application's advanced controls ultimately a greater reliance by the business on its ERP investment. Additionally, the use of advanced controls results in:

- a greater use of automated controls
- a more effective configuration management program
- a more effective regulatory compliance program

Quadrant: Application Security

Organizations continually struggle with good application security controls. Roles and responsibilities typically provide excessive access to users of the ERP. Additionally, when a


Infrastructure Security
Cyber Security
Information Protection
Business and technology Resilience
Data & Infrastructure Security
Role Based Access Controls (RBAC)
Segregation of Duties (SOD)
Authentication
Access Permission Architecture
Application Security
Conversion & Interface Controls
Configuration Controls
ERP
Advanced Controls
Business Process Controls Frameworks
Preventative Controls
Detective Controls
User Access Administration
ERP Security Operations
User Analytics

Source: GRC Today, October 2015, KPMG International

company goes under a re-organization or a merger, roles and responsibilities are often required to be re-engineered to address new or different job positions.

During an ERP implementation, application roles and responsibilities are typically not finalized for user acceptance testing. Even then, roles and responsibilities are typically only developed to support completing business transaction. Detail assessments of security design for compliance with company segregation of duties policies have historically been performed much after go-live.

Application Security: Key Business Drivers

The primary driver of application security is to ensure logical access to the business systems aligned with policy and is controlled a sustainable manner. Application security includes:

- employees access to the applications
- fine grained access to sensitive ERP transactions and data
- reducing risk of fraud and error
- effectively address complex regulatory compliance requirements

Application Security: Focus and Scope

Application security includes concepts of both authentication and authorization. Authentication addresses how each of the applications understands who as associated to each of the user accounts. Authentication includes single sign-on and multi-factor authentication methods such as the use of a security token.

Authorization addresses what privileges are provisioned to each user account. Authorization includes the following items:

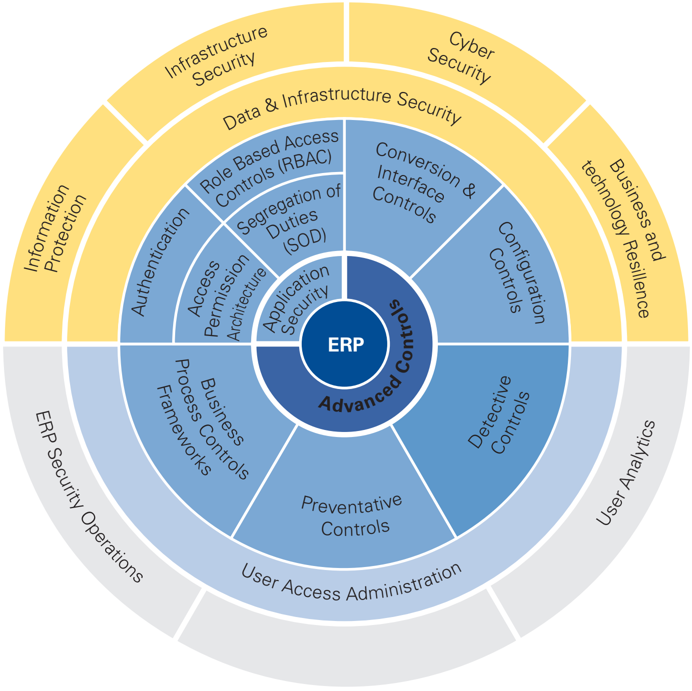
- Role-based access control
- Dynamic access based on user attributes
- Function security – transaction-level access to an ERP
- Data security – access to key data elements
- Operational segregation of duties framework

Application Security: Realized Value

The realized value from Application Security is a better alignment of application access to users' functional job assignments. This alignment along with good control over maintaining the security design helps to reduce costs associated with user administration. Additionally, Application Security is a fundamental area in maintaining an effective compliance framework.

Quadrant: Data & Infrastructure Security

With the recent and massive data breaches of government entities and large commercial organizations, companies are re-evaluating their perimeter security. Additionally, these data breaches have organizations re-evaluating where their data is stored, where it flows, and how that data is kept complete, accurate, and safe. Perimeter and data controls are paramount in keeping the organizations' and their customers' confidential and proprietary information secure.


Infrastructure Security
Cyber Security
Information Protection
Business and technology Resilience
Data & Infrastructure Security
Role Based Access Controls (RBAC)
Segregation of Duties (SOD)
Authentication
Access Permission Architecture
Application Security
Conversion & Interface Controls
Configuration Controls
ERP
Advanced Controls
Business Process Controls Frameworks
Preventative Controls
Detective Controls
User Access Administration
ERP Security Operations
User Analytics

Source: GRC Today, October 2015, KPMG International

Data & Infrastructure: Business Drivers

With the inter-connected nature of how businesses need to operate, the most obvious threat associated infrastructure and data security is the risk of unauthorized external access and theft of information. The compromise and theft could also come from inside the organization. Theft could come directly as a result of attack and penetration activities but also simply through social engineering.

Theft of data is not the only major risk associated with infrastructure and data security. Organizations, due to their global footprint, increasingly require a highly available environment. Even small outages from technology failures could have a measure and negative impact on revenue.

Data & Infrastructure: Focus and Scope

The focus and scope of good data and infrastructure security includes a number of items:

- Data protection program: Organizations need to understand where their sensitive is stored, where it is in transit, and provide the appropriate controls and at the proper level such as data masking, hardened database and networks, and vulnerability management.
- Cyber security program: Organizations should be able to provide defenses, monitor cyber activities, identify breaches, and effectively escalate through and incident response program.
- Business and Technology Resilience program: Organizations are sensitive to disruption to their business. This disruption could affect not only the technology in use but also the organization in general. Initiatives used in this area include system performance monitoring, disaster recover procedures, business continuity management, high availability infrastructure, and crisis management.
- Privileged account management: The management of critical system accounts is imperative to keep and organization's data secure.

Data & Infrastructure: Realized Value

The realized value of data and infrastructure security is a risk-based information security program to protect ERP assets. This program also contributes overall to an effective regulatory compliance initiative.

Quadrant: User Access Administration

Organizations have been focusing on effective user management for many years. Fifteen years ago at the height of the dot.com bubble, organizations were investing heavily in identity management and user access provisioning. The initial focus of this investment was reducing the cost of administering access. Then, organizations were faced with the challenge of understanding and reporting on user access across the enterprise.

User Access Administration: Business Drivers

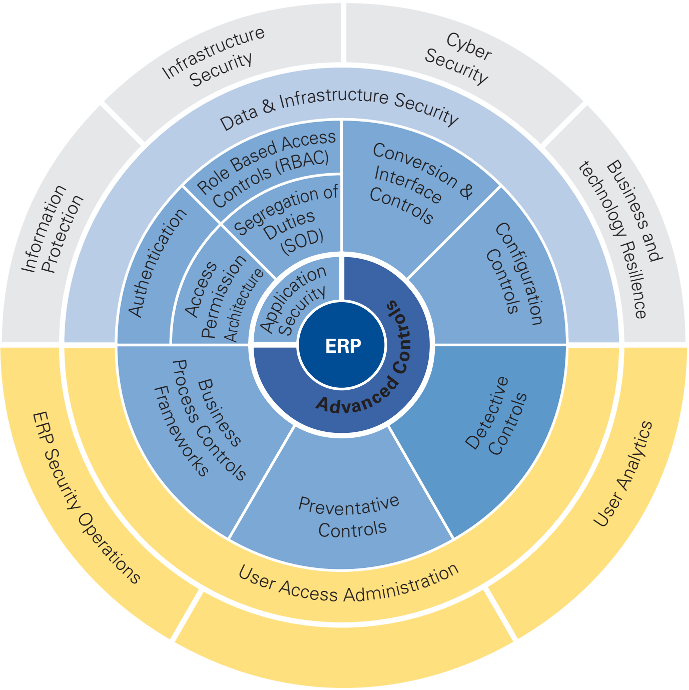
Key business drivers behind user access administration include:

- Lowered cost:
  - Organizations strive to lower the cost of provisioning activities. User provisioning can be a highly automated and dynamic activity if designed and maintained effectively.
  - User access reporting is also a very time consuming and quite often an expensive task. Automating the collection and analysis of user access throughout the enterprise reduces cost and increases the reliance of the associated reporting.
- User activities: Organizations need to have a good understanding of user access to aid in monitoring key business transactions in their ERPs. They also need to have good controls in place to monitor key and privileged users throughout the organization.

User Access Administration: Focus and Scope

The focus and scope of user access administration involves good policies and procedures and effective underlying technology:

- Policies and procedures: Organizations who maintain effective user access administration have good policies and procedures around organizational design, effective governance and reporting, enterprise and user-level segregation of duties, ERP controls enablement strategy and remediation processes.


Infrastructure Security
Cyber Security
Information Protection
Business and technology Resilience
Data & Infrastructure Security
Role Based Access Controls (RBAC)
Conversion & Interface Controls
Authentication
Segregation of Duties (SOD)
Configuration Controls
Access Permission Architecture
Application Security
ERP
Advanced Controls
Business Process Controls Frameworks
Detective Controls
Preventative Controls
ERP Security Operations
User Analytics
User Access Administration

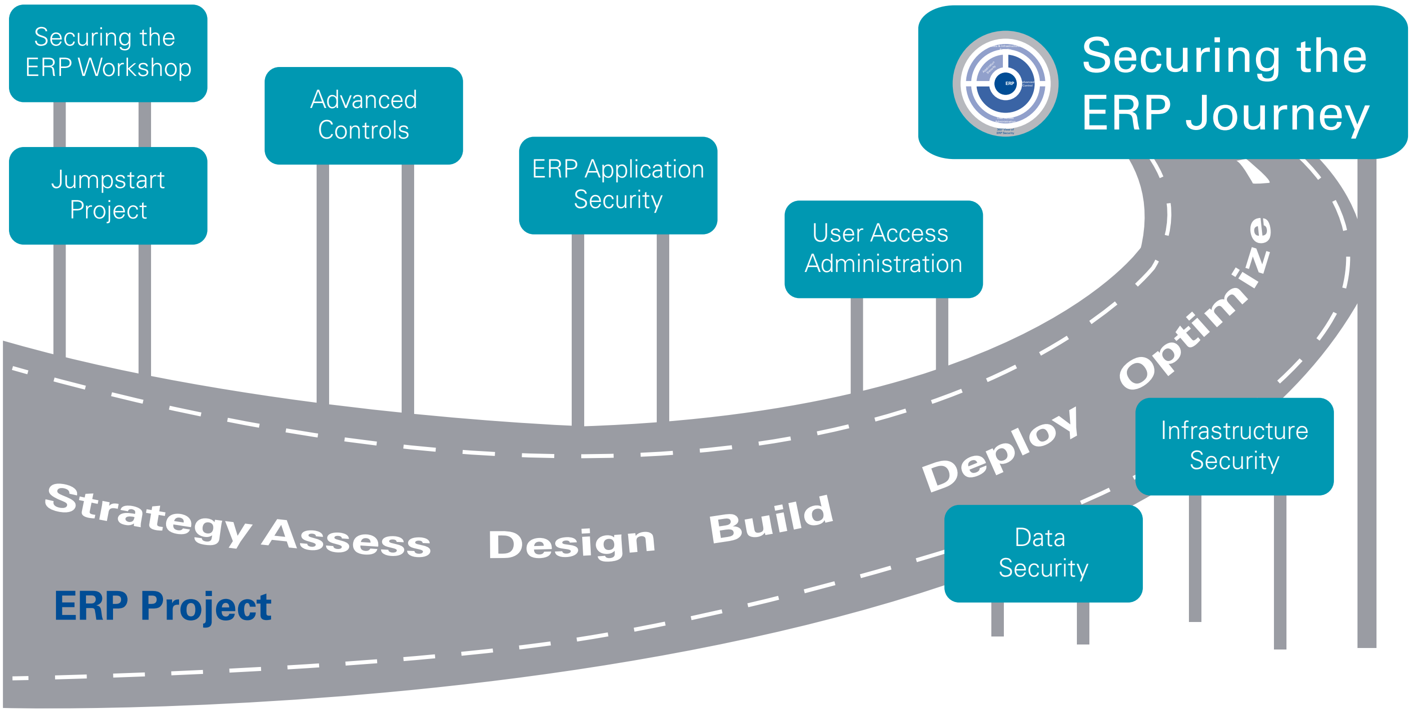
Source: GRC Today, October 2015, KPMG International

- Enabling technologies: Organizations with effective user access management leverage many of the following capabilities in place: Registration, Self Service, automated user provisioning with approvals processes, password management, and account validation.

User Access Administration: Realized Value
The realized value of a good user access administration program is effective ERP user management at a reduced cost. Good user access administration also contributes overall to an effective compliance program.

Securing the ERP Journey

KPMG's Securing the ERP methodology can help organizations meet those additional objectives not fully addressed by the ERP. Leading an organization on a path through its own Securing the ERP journey begins with a single workshop. In this workshop, we educate the client on the aspects of Securing the ERP. We then help the client jumpstart their program and guide them along the path from initial, ad-hoc activities to optimized and automated controls.



Source: GRC Today, October 2015, KPMG International

Case Study – Industrial Manufacturing

Export-controlled information is common in many high-tech manufacturing organizations. These organizations face challenges of where that information is and who can access it. This challenge is a multi-faceted issue involving application controls, infrastructure and cyber security, and user security and administration. KPM was recently engaged with a high-tech manufacturing organization to help them manage their export-controlled information using this Securing the ERP approach.

For more information

Laeeq Ahmed
Advisory Managing Director
GRC Technology, KPMG in the US
E: laeeqahmed@kpmg.com

Brian Jensen
Solution Relationship Director
Market Execution Center
KPMG in the US
E: brianjensen@kpmg.com