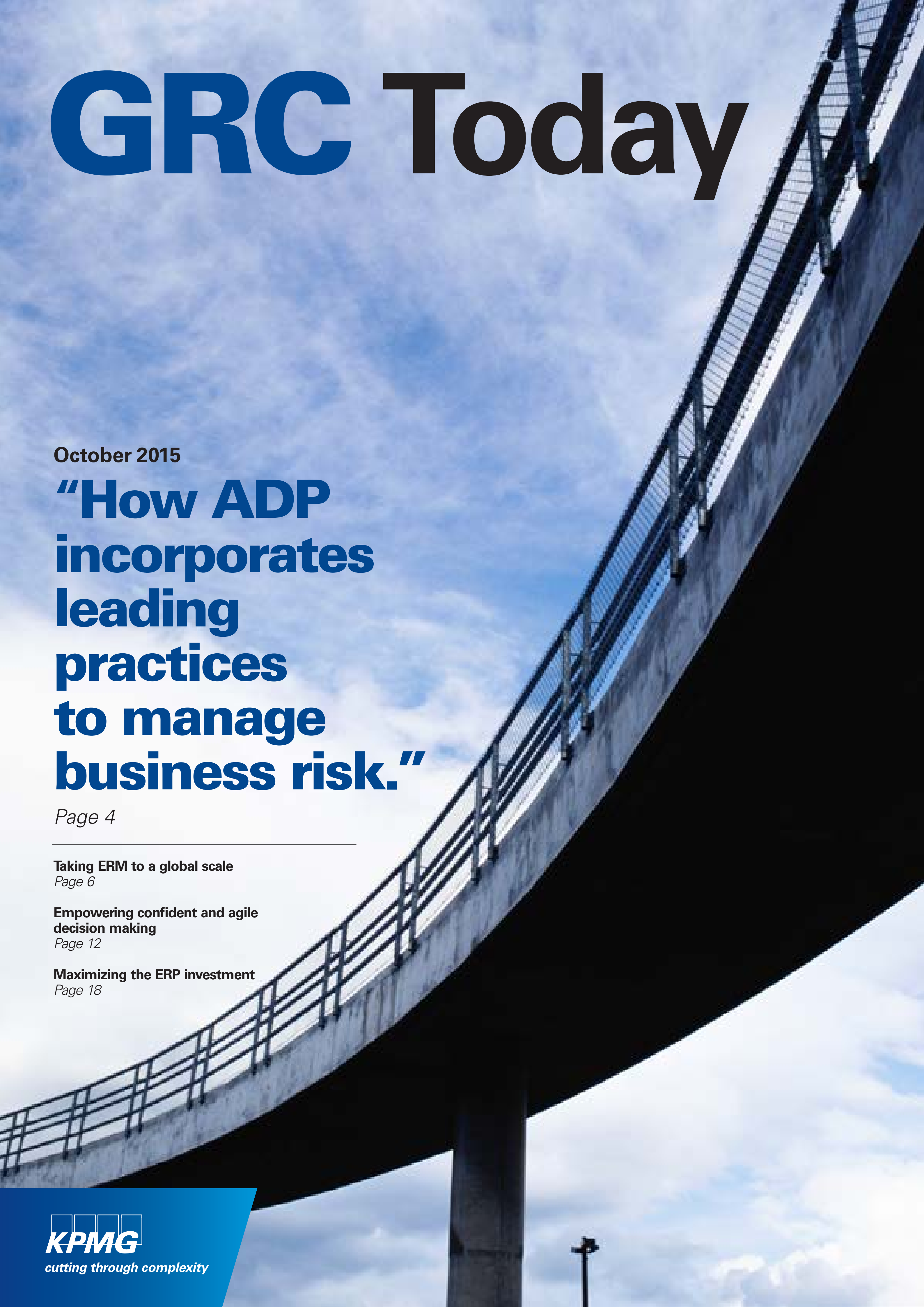
GRC Today



October 2015

“How ADP incorporates leading practices to manage business risk.”

Page 4

KPMG
cutting through complexity

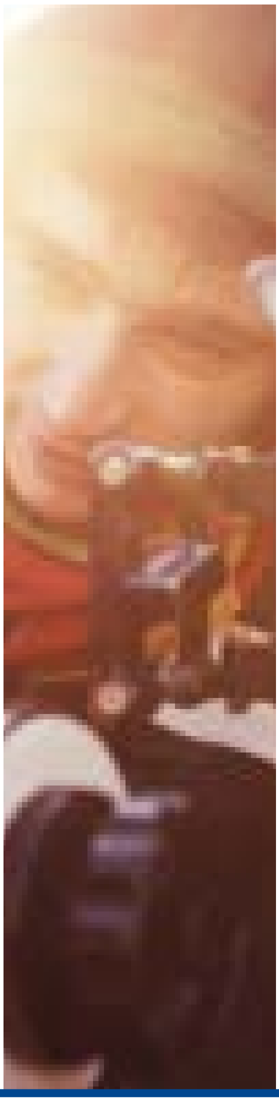
GRC Today:

Insights in Governance, Risk and Compliance.

The GRC Today is an international publication from KPMG's Advisory Risk Consulting practice and seeks to update you on developments in the field of Governance, Risk and Compliance (GRC). Topics include amongst others: new laws and regulations, soft controls, GRC tooling, leading practices and case studies. The GRC Today is distributed to a wide audience to provide insights and food for thought on their GRC journey.

For more information:
KPMG Advisory
grctoday@kpmg.com

Contents



“The Global ERM Framework provides a clear, practical vision that adds business value and builds a competitive advantage by allowing organizations to avoid downside risks while discovering the potential upside within risks.”

“Cumbersome or poorly defined decision review and approval processes can also cause ambiguity and lead to missed opportunities.”

“Organizations demand more from their ERP investments. A successful ERP project will indeed help streamline processes and reduce the overall cost of doing business.”

“Starting with a common taxonomy for risks, controls, and issues, the goal of GRC convergence is to break-down traditional silos and replace this fragmented approach with a single view of risk.”

How ADP incorporates LEADING PRACTICES to manage business risk

ADP vital statistics

- Serves more than 630,000 clients in 100 countries
- Approximately 55,0000 employees worldwide
- Pays 24 million workers in the U.S. and 12 million elsewhere
- Total revenues of $10,9 billion for the fiscal year to end-June 2014
- Net earnings of $1.4 billion for the period

Source: www.adp.com

Automated Data Processing, Inc. (ADP) is a human capital management company based in Roseland, New Jersey, that provides payroll and other HR solutions to thousands of companies globally. Founded in 1949, ADP has long understood the importance of managing its risk. Given the evolving competitive landscape and the emergence of disruptive technologies ADP's ERM program elevates the company's risk awareness, without being seen purely as a 'risk mitigation' program.

Process

Creating a risk aware culture together with common risk language and framework is a leading ERM practice that ADP embraced. To do this, ADP evolved their ERM program based on the foundation that was previously established by management and the Board. This foundation included a 'risk wheel' that incorporated a high-level view of where risk could occur. To evolve the risk management program and not add a bureaucratic layer, senior leadership appointed a vice president, a director and a manager on a full time basis reporting to the Chief Audit Executive.

The ERM team described its vision in terms that indicated it was a business enabler, not a hindrance. When gathering risk information, the team was careful to speak the same business language as the stakeholders they were interviewing as well as explore opportunities where taking measured risks might be beneficial.

The aim of the ERM program is ongoing reinforcement and enablement so that associates think and behave more intelligently about risks, thereby improving business results and strengthening the protection of ADP's reputation. To achieve this, risk management has been embedded in the company's processes and the culture, so that there's a continuous focus on key risks, threats and opportunities.

Governance

Clearly defining accountability is an ERM leading practice and is critical to ensuring that there is a positive adoption of the risk management framework. ADP chose the model of the three lines of defense, with the business clearly understanding that they are the first line of defense, or the risk owners. The second line is composed of corporate functions that have oversight of risk management and control, such as those responsible for data privacy and security, anti-bribery and overall compliance. Internal Audit is the third line of defense.

The ERM team is governed by an ERM Steering Committee that includes Chief Executive Officer and selected other members of Executive Management. The Steering Committee meetings aim to take full advantage of executives' time; they can deeply explore a critical risk or seek to improve ways of using risk metrics to gain a better understanding of leading indicators. Day-to-day risk management resides firmly in the business units. The ERM team provides periodic updates to the Audit Committee or the Board of Directors.

Risk profile lenses

Another leading practice is to ensure the ERM program is aligned with strategic and business objectives and is focused on the threats to them. From the outset of the ERM program, the risk team has worked closely with ADP executives and the Board of Directors to develop the risk profile, including both primary and secondary risks facing the company. In addition, the ERM/Internal Audit team has found it useful to categorize the risks into three main areas, each of which requires a different approach to manage, monitor and audit the risks.

Strategic Risks: These emanate from the major strategic initiatives the company is undertaking or is planning to take. The initiatives often involve investment, changes to the business model, changes to products and services, etc. These initiatives can create new risks that need to be considered in a more strategic way. The role of ERM is to help management to establish good governance and embed the relevant components of the ERM framework into the initiative.

Operational Risks: These include areas such as compliance and data security, where the risks are well-known and the processes long-established. In this category, the risk management practices tend to be more mature and focused on such things as the mechanisms used to monitor operations. ERM can help the business owners improve the ways to monitor their risks by using advanced analytics. It can also help create a more consistent risk process, among other things.

External Risks: These tend to be factors external to the organization that could affect the business, such as new regulations or a disruptive new technology. ERM can help management develop mechanisms to monitor the external risks or facilitate deep dives to define actions that could be taken if the risk materializes at an enterprise level.

Once categorized in these three ways, the identified risks under each heading become the basis for a discussion with senior executives and the Board about corporate strategy and the array of possible threats to the fulfilment of the company's goals.

Measuring and monitoring

Leading companies use data & analytics to enhance the understanding of risk and to improve business decision making. At ADP, the ERM department is evolving its efforts to collect and analyze data in new and powerful ways. There are few things that get more attention from senior executives and the Board than good, useful data. And ADP's risk department's goal is to be adept at data & analytics. They are continually looking for new ways to gain keener insights into the risks, in some cases combining data from various parts of the organization to create a three-dimensional view of risk.

Fitting the culture

The key to ADP's approach to ERM is the way it has adapted risk management to the culture of the company—a "one size fits one" approach. Risk management could have been viewed as a brake on innovation. But the ERM team recognized the importance of understanding the culture and adapted the speed of implementing the ERM program accordingly. If it tried to take a "one size fits all" approach, the ERM program would have failed.

Another leading practice to improve adoption is to develop a common risk framework and language that is used across the enterprise. ADP has created an integrated approach to ERM, by embedding the risk-and-control oversight function into a unified framework that is used by those responsible for data privacy and security, anti-bribery and overall compliance. This allows the second and third lines of defense to view enterprise risks in the same manner and communicate cohesively to the Audit Committee and the Board. But the process is not finished, because ADP is continuously aiming to build a more integrated risk assurance. To enhance consistency, the risk framework created by the ERM team is being communicated to other parts of the company in the form of a risk-management toolkit intended for operating areas and businesses to use to improve their own processes and oversight.

Critical success factors in ADP's risk program

1. Integrate ERM practices into the daily activities of business managers.
2. Aim to be viewed by the business as a facilitator of business value and innovation.
3. Integrate the ERM framework with the other risk-and-control oversight functions to create a unified view of risk.
4. Focus the ERM program on the threats to strategic and business objectives, including missed opportunities.
5. Use data & analytics to enhance the understanding of risk and to improve business decision making.
6. Understand the organization's culture and build an ERM program that evolves along with it.

For more information:

Deon Minnaar
Partner, Risk Consulting
KPMG in the US
E: deonminnaar@kpmg.com

Vishal Mehta
Director Risk Consulting
KPMG in the US
E: vmehta@kpmg.com

Taking **ERM** to a GLOBAL SCALE

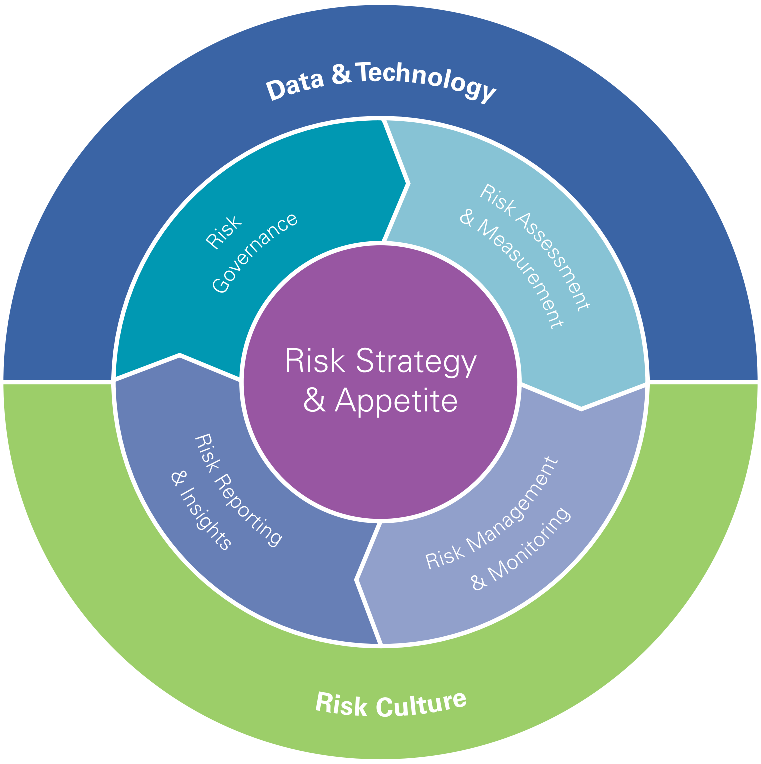
Global events – highlighted by business scandals, failures, information theft, and natural disasters – have shone the spotlight yet again on risk management (or the lack of it!) among investors, owners, boards, stakeholders and customers. The inability of risk systems to protect business assets at critical times has shifted attention to how risk management is embedded into the day-to-day responsibility of everyone at the organizations.

As business leaders attempt to re-invigorate their ERM programs, the need for a robust ERM framework still persists. KPMG has quickly recognized the needs of its member firm clients, the expectations of regulators, and the requirements of the market and proactively issued a fresh and updated version of its original ERM framework. The new Global ERM Framework provides consistency across global markets and applies to all industries. Moreover, the new ERM Framework helps identify risks embedded in corporate strategy, day-to-day business operations and processes and responds to board-level concerns about risk management initiatives, the ability to avoid crises through insight, and the effective evaluation of leading risk indicators.

An Elegant Approach

KPMG member firms take an elegant approach with its new Global ERM Framework and Risk Maturity Continuum. In contrast to the original framework, the new Framework illustrated in figure 1 addresses cultural needs and the maturity of current ERM programs with the addition of the Risk Culture, Risk Appetite and Data & Technology elements. The new Risk Culture element focuses on values and behaviors that shape an organization's ability to manage risk through risk decisions and risk awareness.

Figure 1 – The Global ERM Framework


Data & Technology
Risk Governance
Risk Assessment & Measurement
Risk Strategy & Appetite
Risk Reporting & Insights
Risk Management & Monitoring
Risk Culture

Source: GRC Today, October 2015, KPMG International

> **The Global ERM Framework provides a clear, practical vision that adds business value and builds a competitive advantage by allowing organizations to avoid downside risks while discovering the potential upside within risks.**

Emphasizing risk culture within the new Framework addresses the impact that an organization's culture can have on the prevention of unacceptable risks and the identification of emerging risks.

Building knowledge and understanding of risk at every level leads to the promotion of risk awareness throughout the organizational culture. In turn, embedded risk awareness leads to heightened commitment and a deeper belief in the convergence of business strategy and risk strategy. Individuals have a greater opportunity to think about the need for risk mitigation and the potential upside of risk. Risk management intertwines with performance management as employees work within their normal activities.

Integrating risk culture, risk appetite, and risk strategy within the new Framework redefines enterprise risk management and highlights openness, transparency, and accountability. When all parts of a business identify, elevate, and manage risk at strategic, operational, and tactical levels, the business – as a whole – can leverage ERM to create value. This increase in value may occur by decreasing the cost of risk, through controlled growth, by mitigating risk ahead of the competition, or by assuming more risk at critical decision-points.

The Global ERM Framework provides a clear, practical vision that adds business value and builds a competitive advantage by allowing organizations to avoid downside risks while discovering the potential upside within risks. Because the interrelated elements and components of the new Framework align risk strategy with business strategy, management gains an understanding of risk strategy, risk appetite, and risk culture at the outset. This understanding nurtures the capability to recognize that new challenges may appear at any time.

Updated Elements And Components

Figure 2 demonstrates the relationship between the updated elements and components found in the new Framework. The updated grouping of the elements and components that make up the new Framework showcases KPMG's dedication to developing sustainable enterprise risk programs and sets a new standard for ERM methodology. Within risk governance, the Framework aligns decision support, strategic objectives, and company structure. This holistic approach to ERM provides a risk operating structure that represents each functional area.

Figure 2 – Elements of the Global ERM Framework

Risk Strategy & Appetite	Risk Governance	Risk Culture	Risk Assessment & Measurement	Risk Management & Monitoring	Risk Reporting & Insights	Data & Technology
Linkage to Corporate Strategy	Board Oversight & Committee	Knowledge & Understanding	Risk Definition & Texonomy	Risk Mitigation Response & Action Plans	Risk Reporting	Data Quality & Governance
Risk Strategy	Company Risk Operating Structure	Belief & Commitment	Risk Identification	Testing, Validation & Management's Assurance	Business/ Operational Requirements	Risk Analytics
Risk Appetite & Tolerance	Risk Guidance	Competencies & Context	Assessment & Prioritization	Monitoring	External Requirements	Technology Enablement
	Roles & Responsibilities	Action & Determination	Quantitative Methods & Modeling	Risk in Projects/ Initiatives		
	Decision Support		Risk Aggregation Correlation & Concentration			
			Scenario Analysis & Stress Testing			
			Capital & Performance Management			

Source: GRC Today, October 2015, KPMG International

With its advantages of experience and expertise, KPMG's network of firms works within the seven risk elements to facilitate and perform an enterprise-wide risk assessment that identifies and measures risk tolerance and risk appetite. The application of the risk elements also provides the basis for KPMG's review and assessment of the linkage between corporate strategy and risk strategy. Through the use of the Global ERM Framework, KPMG's network of firms can tailor a risk program to particular needs.

With the combination of the Risk Strategy and Risk Appetite elements, KPMG's teams effectively anchors risk appetite within the organization's strategy and guides organizational governance. A risk appetite statement identifies major risks, defines acceptable levels for major areas of risk, and articulates the motivation for taking or avoiding risk. Placing a clear and concise risk appetite statement within the organizational strategy aligns risk appetite with the organization's values, strategic objectives, and business decisions while recognizing the diverse interests of all stakeholders. By grouping risk strategy, risk appetite, and risk tolerance, KPMG's network of firms establishes boundaries for the amount of risk that an organization will accept within quantitative and qualitative measures of loss at the enterprise and operating unit levels. The emphasis on risk management, monitoring, and reporting within the new Framework connects risks and controls with financial performance and strategic objectives. Management may receive requests to validate the capabilities of their organization's processes that mitigate existing and emerging risks. In response, a board or stakeholders may use this information to assess the relationship between returns and risk.

The new Framework increases risk management capabilities through three lines of defense that include the continued monitoring of internal and external risks, the integrated guidance for monitoring activities, and the active monitoring of risk exposure. Risk reporting occurs across the areas within business units and focuses on support for decision-making. With a meaningful risk culture in place, the implementation of risk assessment and risk measurement supports strategy and decision-making through the application of a well-defined risk taxonomy and identification system.

Continuous Risk Management

The Framework supports continuous risk management through the components found within the Data & Technology Element. Tools and processes within the Data & Technology element combine to reinforce a risk aware culture and the three lines of defense model. Technologies formed around the use of big data allow employees at all levels to analyze the output of predictive models and to search for patterns. The application of timely, accurate data from a variety of sources combined with data visualization tools drives advanced assessments of risks and allows board members to make informed and faster decisions. Because big data includes historical and real-time data from external and internal sources, the analysis helps inform a broad view of risk inventory and risk appetite.

The individualized approach advocated by KPMG recognizes that some risks align better with quantifiable metrics while other difficult-to-measure risks require a qualitative approach. Utilizing quantitative, numerical analyses of common, structured data allows the monitoring of the health of the business, the identification and solving of problems, and the recognition of opportunities. Qualitative analyses of an increasing amount of unstructured data provide a continual stream of critical insights into current and emerging risks as well as opportunities for capturing increased revenues.

The Risk Maturity Continuum

With the inclusion of an expanded Risk Maturity Continuum scale, KPMG separates the Global ERM Framework from other ERM models. The Continuum scale applies a consistent assessment of maturity to global clients of all levels and across various industries. Referring to figure three, the seven elements of the Framework reach across the five levels of the Risk Maturity Continuum scale.

A risk maturity assessment considers peer companies and industry best practices while identifying changes within structure, governance, policies, and tools that will close performance gaps. The assessment also includes estimates about the amount of time, effort, and financial investment needed to reach different stages of maturity. For example, an assessment may conclude that an organization has sustainable maturity because the business does the minimum to meet the expectations of internal and external stakeholders while defining some risk management strategies. Applying external benchmarking along with measurement and monitoring through the Risk Maturity Continuum identifies emerging risks and establishes continuous risk assessment.

Achieving Value

A well-designed and executed ERM serves as a crucial part of strategy-setting because of the close alignment of risk management with the achievement of objectives. The Global ERM Framework:

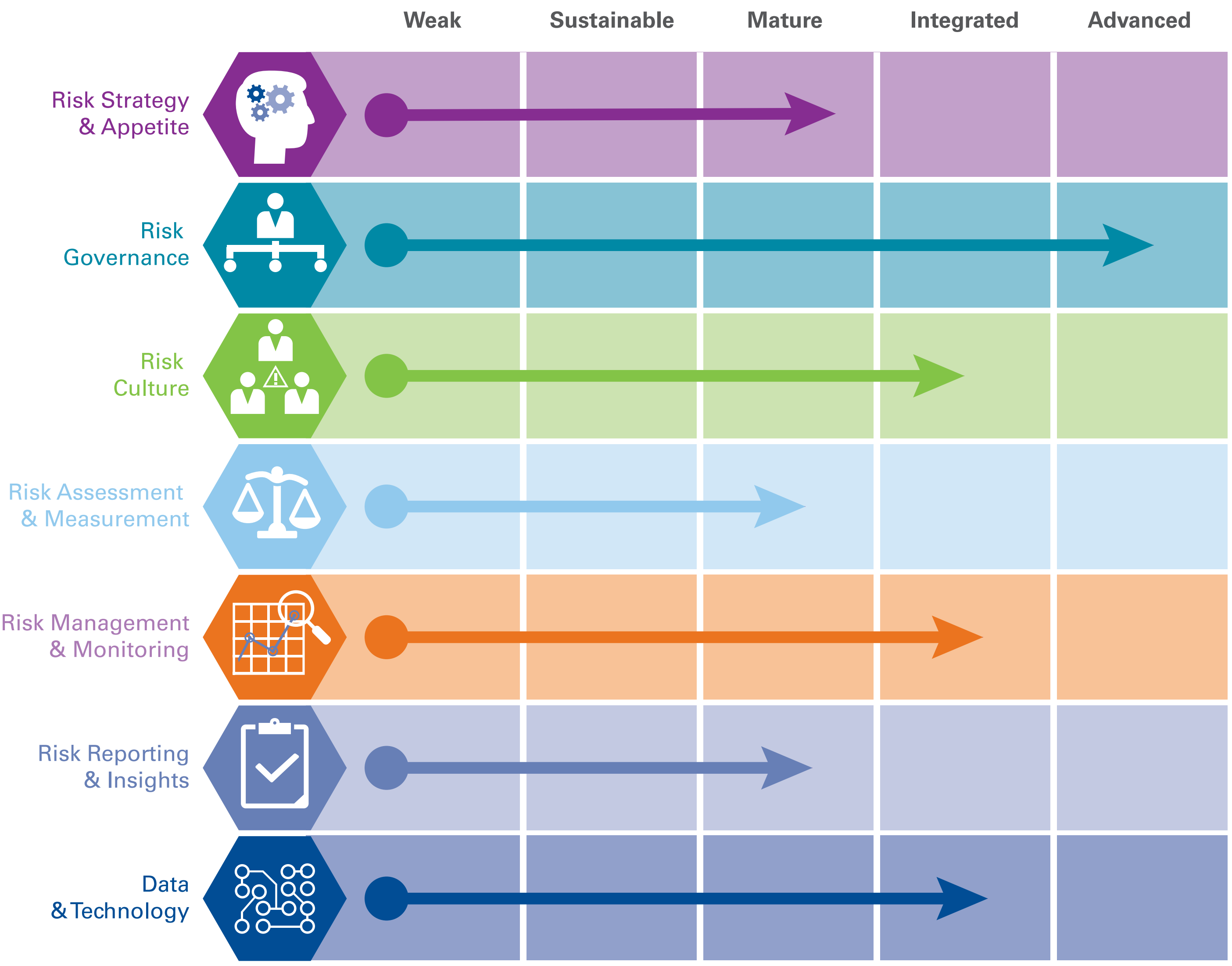
- aligns risk strategy with business strategy;
- recognizes the value of the risk culture;
- manages risk within the risk appetite of the organization;
- identifies potential events that affect the success of the organization; and
- utilizes advanced analytics to provide oversight and control.

These and other factors drive the continuous improvement of risk management capabilities.

In addition the application of KPMG's Global ERM Framework reassures board members that management deploys a solid risk management strategy to achieve business results. The emphasis on risk culture, risk strategy, and risk appetite improves risk awareness and encourages transparency throughout the organization. Interrelated elements and components provide an ongoing process that flows through an organization and allows contributions at every level.

An understanding risk strategy and risk appetite drives performance, value, and brand. Principles defined within the

Figure 3 – Global ERM Framework Risk Maturity Continuum



Source: GRC Today, October 2015, KPMG International

Global ERM Framework encourage all stakeholders to understand business strategies and related risks as they implement processes and tailor-made solutions that improve the risk maturity of the organization. The Framework aligns with strategic objectives and organizational risks while incorporating practical approaches to embedding ERM within the organization. Applying the Global ERM Framework and Risk Maturity Continuum improves risk information by consistently identifying and assessing risks through the measurement, reporting, and monitoring of processes.

For more information:

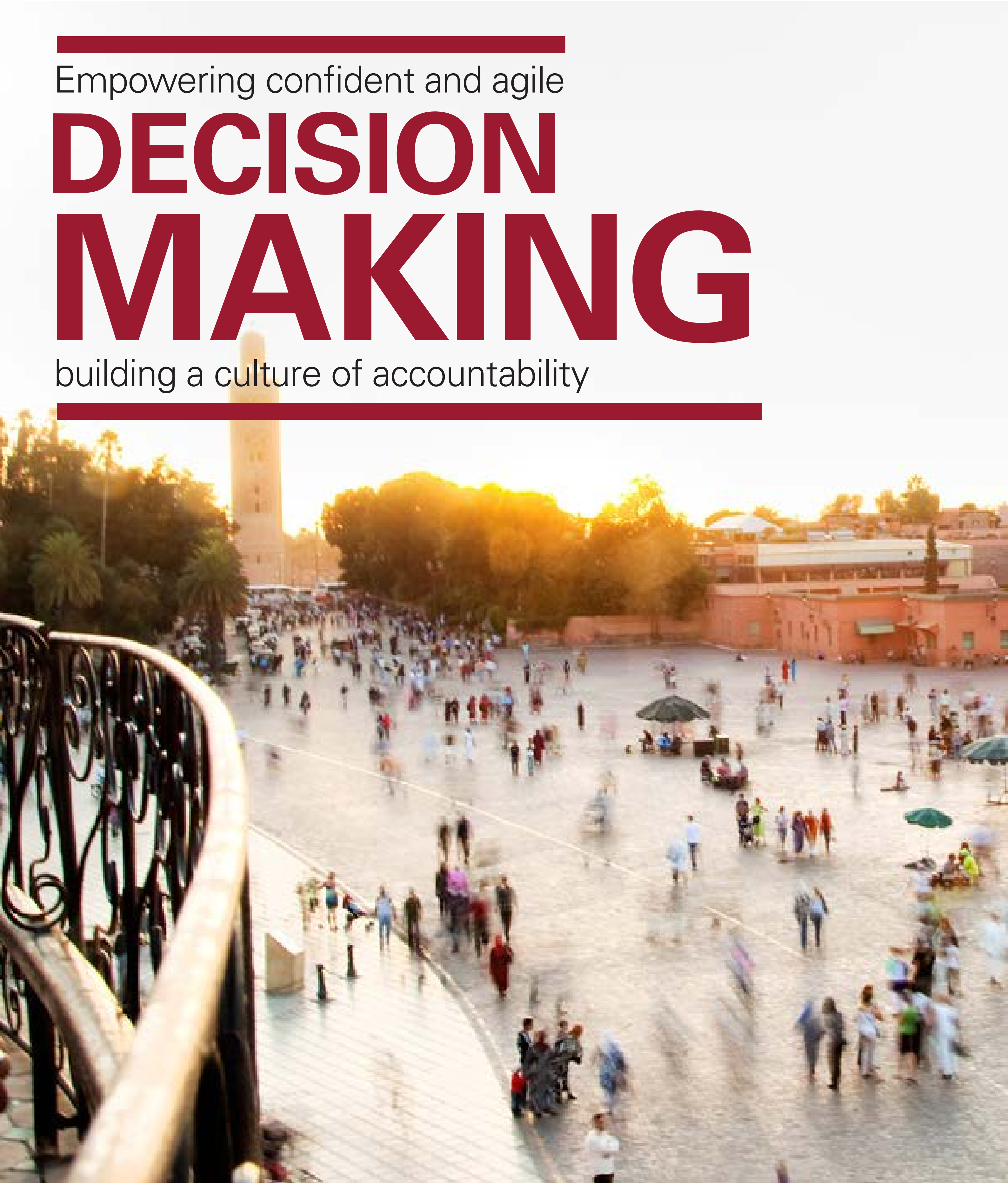
Deon Minnaar
Partner, Risk Consulting
KPMG in the US
E: deonminnaar@kpmg.com

Vishal Mehta
Director Risk Consulting
KPMG in the US
E: vmehta@kpmg.com

Empowering confident and agile

DECISION MAKING

building a culture of accountability



Every day, thousands if not millions of decisions are made by individuals and teams within businesses. Experience, qualifications, gender, age, culture, personalities and health factors (e.g. stress levels, sleep patterns) all play a part in the way those decisions and choices are made.

While many decisions are routine in nature (i.e. have been performed before with precedents to draw from), there are many that are non-routine or ad-hoc (i.e. there are fewer collective experiences to draw from). These are the times when individuals typically draw from their own experiences to solve problems.

So how can the board, management and key stakeholders remain assured that decisions being made across the company are in accordance with the company's (rather than individual) objectives and values and in the best interests of shareholders?

As a starting point, companies are required to establish a constitution or articles of association that set out, at a high-level, what the company must do to satisfy legislative and regulatory requirements, including the power vested to the board. However, these do not typically provide practical guidance to personnel in making decisions in every-day activities.

As such, many companies have established delegations of authority and policies and procedures to set out expected behaviours and limits for making/approving decisions. Some companies go a step further by developing risk appetite/risk tolerance limits to define and guide decision making.

Yet these mechanisms have failed to prevent breaches of authorities from occurring, leading to serious adverse exposures for the company.

For example, there have been many instances (particularly prior to the global financial crisis) where investment bank traders circumvented trading limits to seek potentially larger gains. While there

> **Cumbersome or poorly defined decision review and approval processes can also cause ambiguity and lead to missed opportunities.**

has been much analysis on the root causes, a key observation is that there was a misalignment of actions with risk appetite and a culture that failed to hold rogue traders to account.

At the other end of the risk spectrum, cumbersome or poorly defined decision review and approval processes can also cause ambiguity and lead to missed opportunities.

For example, a not for profit organization identified a commercial property that would be suitable to invest excess funds (from sale of land and buildings). However, the existing constitution was silent on whether such a transaction required board approval. The board and management requested a change to the constitution to clarify allowable transactions. However, during the time taken to amend the constitution, the commercial investment property was no longer available and the opportunity was lost.

If a clear decision-making hierarchy is important, what is holding organizations back from establishing it more effectively?

What are the key challenges?

Delegating authority is the process and mechanism to allocate powers to make decisions (or seek approval in advance), ultimately from the board level cascaded to the CEO, executives, management and throughout the company. Delegations of authority are a key pillar of corporate governance and provide an internal control that clearly defines accountabilities, generates consistency in approval mechanisms, manages expectations and prevents unauthorized decisions.

However, there are challenges in establishing adequate and effective delegations of authority including:

- **Scope** – for a number of companies delegations of authority remain as financial approval limits and legal/

contractual sign offs only. But what about critical strategic and operational decisions such as closing a division or plant, appointing nominee directors etc?

- **Level of detail –** determining the appropriate level of granularity can be difficult in practice. For example, delegations that are too high level may lead to gaps and ambiguity; too much detail may lead to inefficiencies.
- **Relevance –** as companies grow and expand over time, the delegations of authorities and key policies may become outdated and misaligned with the company size, scope and nature of operations.
- **Applicability –** establishing a process to determine the applicability of authority limits across company structures and locations can be challenging, particularly where conflicts with local policies and delegations may occur.

In practice, companies are beginning to devote time to enhancing their existing delegations of authorities and have started to recognise that it is important to supplement the authority limits by establishing guiding principles of risk appetite/risk tolerance.

Risk appetite is the amount of risk a company is willing to take in pursuit of strategic objectives. Risk tolerance limits set out how much risk the company is willing to accept.

For some industries (such as financial services) and/or markets these concepts are mandated and well established, for others they are an emerging area of practice to date. Some of the key challenges (predominantly for non-financial services companies) related to risk appetite/tolerance include:

- **Clarity of concept –** for some industries and companies, the concept of risk appetite/risk tolerance is a fairly new one. As such, it may take time for it to be well understood and adopted as a decision making tool.

- **Metrics** – the ability to identify, measure and monitor the right areas of risk can be challenging due in part to poorly defined and communicated strategies and risks.
- **Data points** – inability to obtain relevant quantitative data points in an efficient manner to measure risk tolerance metrics.
- **Oversight** – where data is not readily available and required to be collated manually, this may impact the accuracy and timeliness of monitoring processes.

Too often in practice delegations of authority and risk appetite/tolerance limits are not always developed and reviewed in a coordinated manner resulting in confusion and potentially outdated or incomplete approval limits.

Furthermore, where delegations of authority and risk appetite are developed in isolation from strategy, they may impact the ability for the business to thrive. Delegations/risk limits that are too low level (and require multiple approvals) impact the agility and speed of decision making. Delegations/risk limits that are too high level may lead to unnecessary/excessive expenditure or sub-optimal decisions being made (due to inadequate consultation and awareness at senior levels) prior to the decision being executed.

In practice, very few companies have established a holistic, integrated and dynamic accountabilities framework that links strategy, risk appetite and authority limits with company values, changing risk profiles, oversight and monitoring functions and clear consequence management procedures.

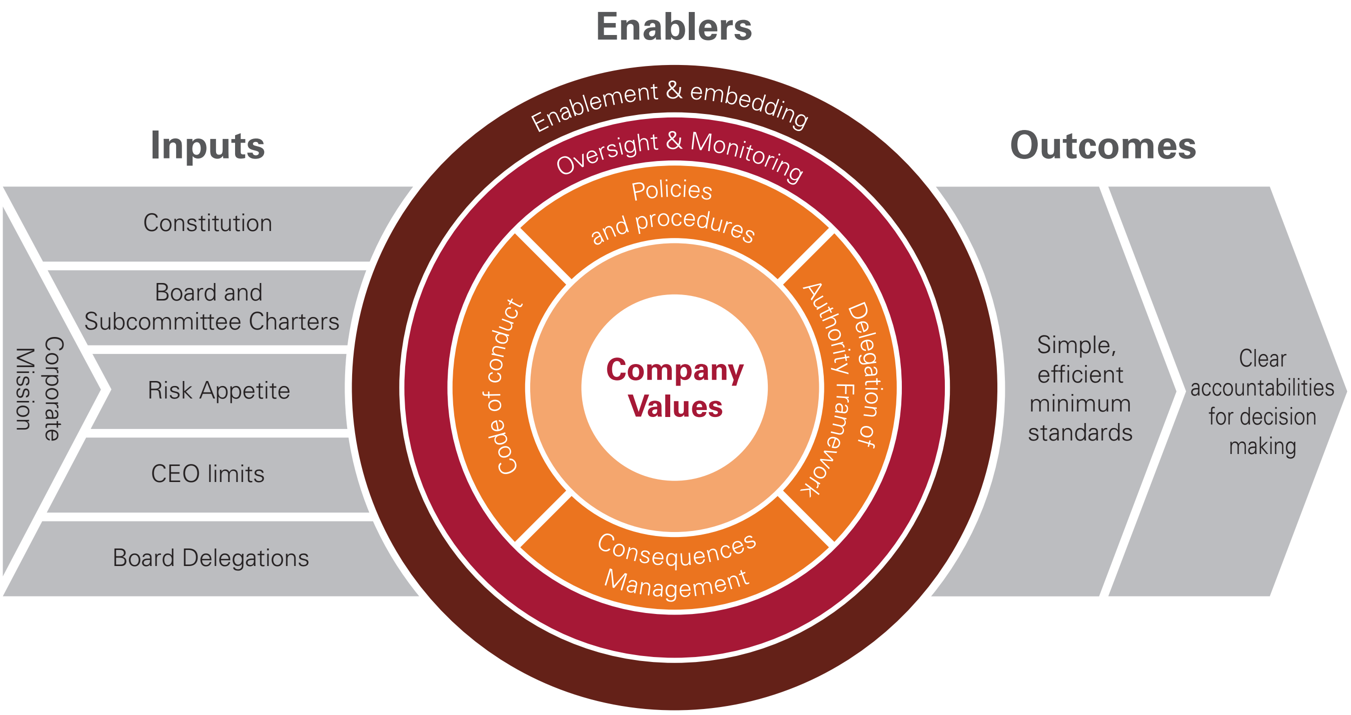
This represents a missed opportunity, a competitive advantage lost. Companies that are able to build an adequate, effective and efficient decision making model are able to move faster, seize opportunities and respond to crises more confidently and consistently. Where employees have clarity of roles and responsibilities, they feel empowered and supported, which is an increasingly critical factor in talent retention.

So what can companies do to address these shortcomings?

The first step is to recognize the interconnectivity between existing key control mechanisms across the organization wide accountabilities framework. All layers in the company need to be empowered, briefed and coached on decision making protocols to provide autonomy and speed when required with the necessary checks and balances.

The key elements are outlined below in the KPMG Accountabilities Framework below.

Figure 4 – KPMG Accountabilities Frameworks



Source: GRC Today, October 2015, KPMG International

Having an accountability framework aligns the key **inputs**, and is critical in setting expected behaviours for decision making, such as the strategy (corporate mission), company constitution (articles of association), terms of reference for boards/board committees, risk appetite and delegations of authority.

However, these are pointless without an effective set of **enablers** to operationalize and embed expected behaviours. Company values form the foundation of the accountability framework. While values may vary from one company to another, understanding what they are is critical as they shape and inform key aspects of the accountability model, including the style in which they are defined, deployed and embedded. Other enablers include consideration of the company operating model. This is particularly relevant as business models, structures (e.g. group and subsidiaries) and locations (e.g. local and multi-jurisdictional) expand and evolve.

The oversight and monitoring framework is critical to identifying and reporting breaches. Part of this involves the processes to identify and evaluate the root causes of the breaches to enable appropriate resolution of matters and/or disciplinary actions to be taken.

It is important to distinguish whether a breach of authority was due to a poorly designed authority limit (i.e. it does not exist or does not address the key risk area), a lapse in controls (such as the person not being aware of the limits or not being trained in complying with the limits) or whether it was a deliberate breach.

Such analysis enables the framework to be continuously improved. Critical to the success of the accountabilities framework is establishing strong 'tone at the top', particularly in deploying the consequence management protocols in a transparent manner.

For example, if the top sales manager was found to have significantly breached an authority limit, and the consequences required the manager to fired, the board and management need to adhere to the protocols regardless of potential lost sales/impact to the business. This is to send a consistent message to the organization that breaches are not tolerated and to demonstrate a strong tone at the top.

The objective of establishing a holistic and integrated framework is to generate **outcomes** that promote practical and simple standards and clear accountabilities for decision making.

Given the importance of these control mechanisms, assigning a function (or champion) to lead/govern the accountabilities framework activities is essential. Equally, it is important to regularly review the framework to ensure its relevance and to make adjustments in response to significant changes in the risk profile and/or external/internal environment.

Decisions are at the heart of everything we do. Establishing structures and processes around the decision making process should not be seen as stifling diversity in thinking but rather enabling decisions to be made with greater confidence, trust and agility.

Delineating clear authority levels provides the basis for well-made decisions at all levels of the organization, which are in turn a critical element of building long term sustainable success.

For more information

Emilie Williams
Director, Risk Consulting
KPMG in Singapore
E: emiliewilliams@kpmg.com.sg

Irving Low
Head of Risk Consulting
KPMG in Singapore
E: irvinglow@kpmg.com.sg

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:

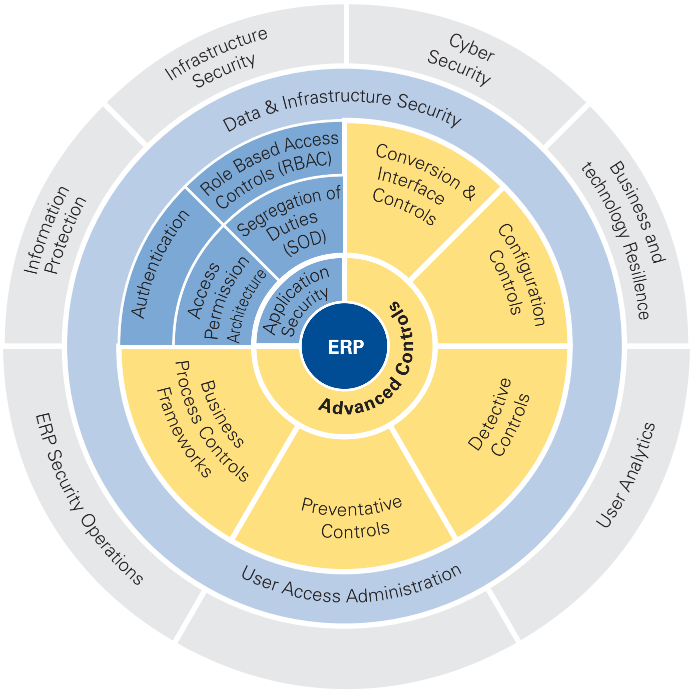
- Improvement for complex and inefficient ERP-centric processes
- lost revenue
- cash leakage
- high configuration and maintenance costs
- greater transparency over sensitive transactions
- reducing the risk for fraud and error

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

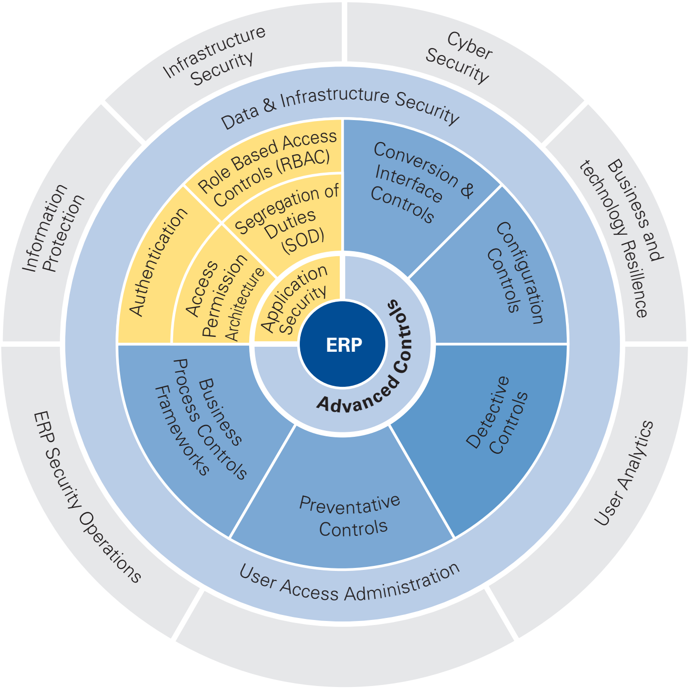
Advanced Controls: Realized Value

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
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

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:

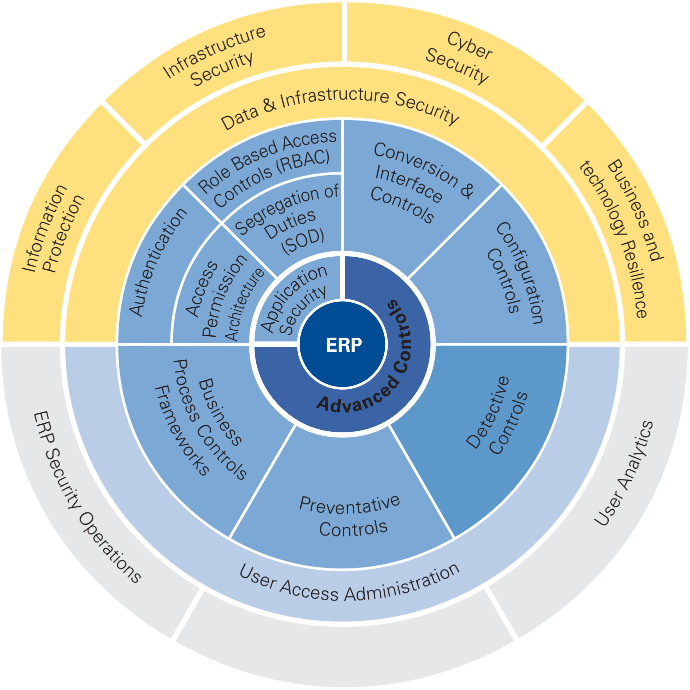
- Role-based access control
- Dynamic access based on user attributes
- Function security – transaction-level access to an ERP
- Data security – access to key data elements
- Operational segregation of duties framework

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
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

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

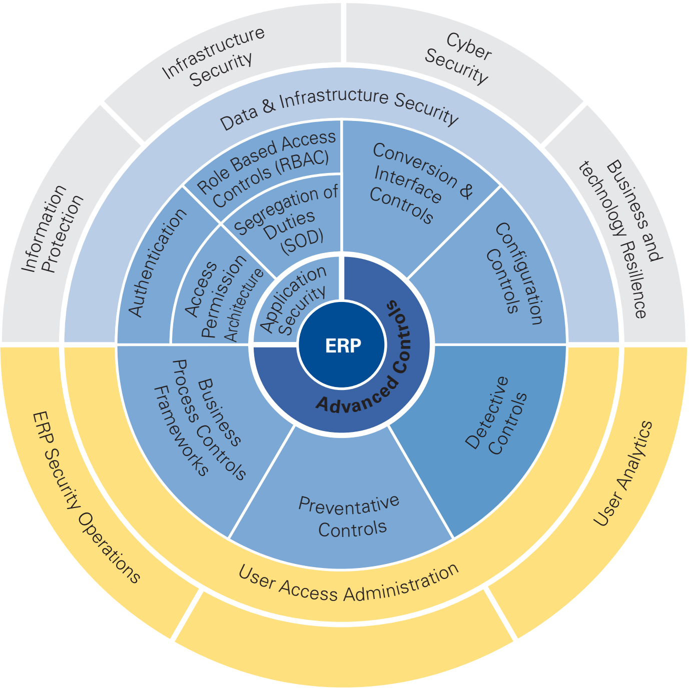
Key business drivers behind user access administration include:

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

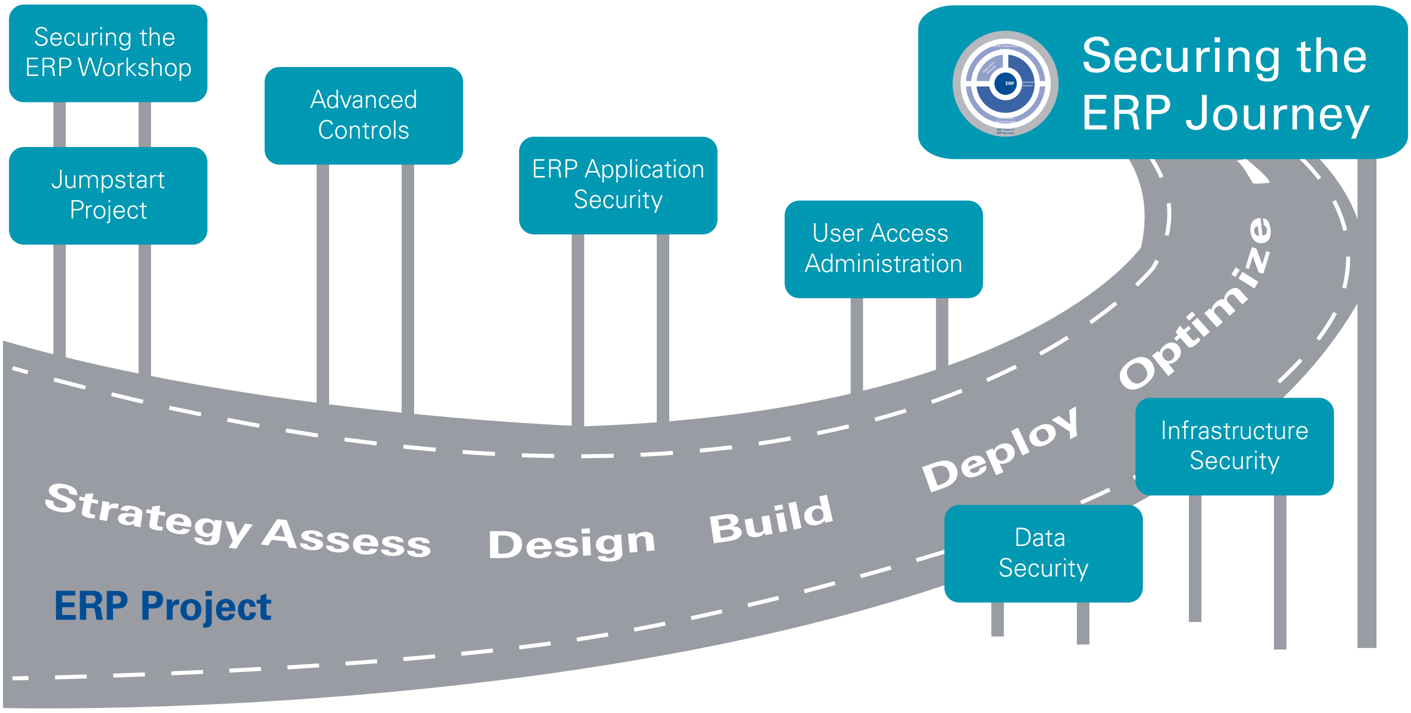
Source: GRC Today, October 2015, KPMG International

- 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

GRC and the ART of FILMMAKING

A film takes us on a journey, a deliberate experience that offers us ways of seeing and feeling that we find deeply gratifying. But this "Art" has some unusual traits – more than other arts. Films are a culmination of complex technology, teamwork among many participants who must follow well-proven work routines, and prudent financial planning. All these elements shape and sustain film as an Art. Similarly, GRC is also a journey, one that requires careful planning, collaboration among multiple business areas, convergence of disparate processes, as well as a technology platform to enable and sustain the program.

As someone who dabbled in film school for a brief period, I routinely managed to ruin seemingly straightforward "shots" by failing to adhere to certain fundamental principles of the Art. However, as an experienced GRC practitioner, I have diligently compiled the missteps and false starts from each of my implementation experience to ensure that I avoid them in the future. Below, we share with you some key insights to positively impact your GRC journey.

Have a GRC Vision

Start with a desired end-state in mind. Develop a GRC strategy and a high-level, execution road-map to ensure your GRC vision drives the implementation and not the tool (which is often the case!). The vision statement helps articulate the value of the initiative to the organization – use action words such as "effective" [risk governance] or "efficient" [risk monitoring] or "standardize" [assurance processes], as well as develop guiding principles that complement the vision – to facilitate broader acceptance and adoption of GRC. This planning exercise will also enable the organization to understand its key challenges, as well as to adapt and innovate in response, rather than customize the tool. In addition, conduct a maturity assessment and consider the readiness of risk/assurance processes that are migrating onto a unified GRC platform. This will drive an efficient and successful GRC implementation.

Integrate, not Just Automate

Be smart and use the GRC tool to drive efficiency and reduce cost of risk and control oversight through integration and convergence. Starting with a common taxonomy for risks, controls, and issues, the goal of GRC convergence is to break-down traditional silos and replace this fragmented approach with a single view of risk. This allows the various oversight functions to better leverage risk information, prioritize risks using a common framework, and most importantly, present a homogenous risk landscape to the leadership team, board and other stakeholders. In addition, enabling a converged view of risk through a GRC technology drives efficiency through automated workflows and configurable controls monitoring.

Companies with existing GRC processes should also examine them and identify opportunities to reduce overlap and eliminate redundancies and help ensure they are maximizing the functionality of existing implementations.

> **Starting with a common taxonomy for risks, controls, and issues, the goal of GRC convergence is to break-down traditional silos and replace this fragmented approach with a single view of risk**

Plan for Change

The GRC implementation is a transformational initiative and like all others of its kind, it will progress through a cycle of initial disruption and suspicion, gradual understanding to formal adoption. However, this progression will not happen naturally. It will need an upfront acknowledgement that there will be resistance to the change and a comprehensive outreach and communication plan in response. Driving GRC program goals requires continuous communication and education and therefore, creating a standalone change management workstream as part of your GRC roadmap is of critical importance. Stakeholders often express confusion about the timing of the roll-out and the impact on their daily work. Some may even see GRC as a threat. Meeting this challenge requires understanding your stakeholders, stratifying them by their degree of understanding and appreciation for the initiative and developing an appropriate change management strategy. Communicating frequently and using different forums – town halls, intranet, emails, group sessions, focused trainings – all are equally important to stay connected with your ultimate user-group.

Demonstrate Success, Early

Nothing succeeds like success and this applies to GRC implementations as well! At a minimum it makes for positive communication and significantly reduces the degree of "hard sell." In order to ensure early success, select a mature process, such as SOX or Internal Audit to implement first. Typically, these processes already have stable and formal workflows, a rationalized set of risks and controls, as well as reporting dashboards that provide the appropriate catalyst for broader discussions related to foundational elements (organizational hierarchy, common language, etc.), and points of integration and convergence.

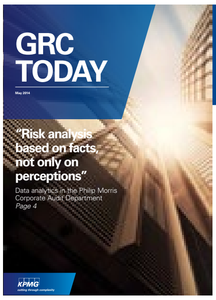
Build for the Future

Take an extended view and identify opportunities beyond converging control and compliance that may benefit the organization. For example, consider on boarding a non-traditional process such as vendor risk. The larger the stakeholder pool, stronger the foundation, and more sustainable the GRC program.

In my closing comments, I would like to highlight an important lesson from cinema – Motion pictures have evolved over the last 125 years through many discoveries in various scientific and industrial fields and continue to do so. Similarly, the GRC program must keep pace and stay relevant, adapting to changes in an organization's business environment or operating model.

Kind regards,
Deon Minnaar, KPMG in the US

Supplementary reading materials


GRC TODAY
"Risk analysis based on facts, not only on perceptions"
Data analytics in the Philip Morris Corporate Audit Department
Page 4
KPMG

GRC Today magazine May 2014

Data Analytics in the Philip Morris Corporate Audit Department

Risk Appetite

Risk Dashboarding

Governance Analytics

Vital Risk Insights

Using business intelligence software to monitor indicators of governance, risk and compliance

The Business Codes of the Fortune Global 200

What the largest companies in the world say and do

Editorial Team:

Marieke Broeders
KPMG in the Netherlands

Jeroen Bolt
KPMG in the Netherlands

Steven Briers
KPMG in South Africa

Mira Rengersen
KPMG in the Netherlands

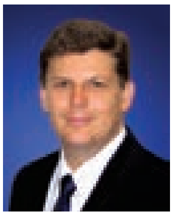
Contact us

Contacts Europe, Middle, East Africa:

Peter Paul Brouwers
Head of Risk Consulting
KPMG in the Netherlands
E: brouwers.peterpaul@kpmg.nl

Bart van Loon
Partner, Risk Consulting
KPMG in the Netherlands
E: vanloon.bart@kpmg.nl

Contacts Americas:



Deon Minnaar
Partner, Risk Consulting
KPMG in the US
E: deonminnaar@kpmg.com

Antonio Torchia
Partner, Risk Consulting
KPMG in the US
E: atorchia@kpmg.com

Contacts Asia Pacific:

Irving Low
Head of Risk Consulting
KPMG in Singapore
E: irvinglow@kpmg.com.sg

Bradley Styles
Partner, Risk Consulting
KPMG in Singapore
E: bradstyles@kpmg.com.sg

kpmg.com

kpmg.com/socialmedia

kpmg.com/app

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by Evalueserve. Publication name: GRC Today. Publication number: 132444-G Publication date: October 2015.