Digital technologies, the rise of mobile commerce and changing consumer behaviour continue to drive transformation in the technology, media and telecommunications (TMT) industry. Providers are focusing on innovative offerings, managed services and cloud services for growth, while also capturing revenue opportunities from new ways in which services are consumed. At the same time, there is an increased focus on optimising operating costs and changing their business models, in part through transformation initiatives designed to improve efficiency, while enhancing the effectiveness of back-office functions.

So how should risk and internal audit functions respond to this changing environment and continue to remain effective? This paper discusses some of the considerations that should be top of the agenda for 2017.

**Building an effective risk management system**

We have observed that companies in the region are continuing to invest in developing their corporate governance and risk management practices, driven to a large extent by regulatory requirements and increased focus by board directors and senior executives.

Responding to these new expectations requires that companies adopt a structured approach to risk management. The key features of such an approach should include:

**Developing a framework**

*How should risk management work in the organisation?*

Develop a sustainable risk management framework that defines how risk management will work in the business. This sets the policy, oversight mechanisms, assessment criteria, risk monitoring and reporting mechanisms.

**Developing content**

*Which risks should the organisation be prioritising and managing?*

Evaluate the strategy and operating environment to develop a holistic view of risk facing the business. Then use the risk management framework to prioritise the top risks needing management focus and attention.
Consistent risk framework and process

Many companies have already invested in a variety of risk management processes, but these mechanisms often lack a unifying vision and clear objectives. Consequently, the potential benefits of good risk management remain unrealised. Presented here are the top five imperatives to help develop a basic risk management framework:

- **Imperative 1** Establish risk management as a boardroom agenda item and provide boards with insights on the top risks facing the business.
- **Imperative 2** Establish a risk appetite to define the level and type of risk the business is willing to accept, and use it to drive strategic decisions.
- **Imperative 3** Develop and roll out enterprise-wide risk management to identify, manage and report on risks to achieving the business objectives.
- **Imperative 4** Define clear accountabilities for the management and oversight of risks across the business.
- **Imperative 5** Set up an internal audit function to provide independent assurance over the effectiveness of risk management and internal control.

Top risk considerations

We often find companies with mature risk management frameworks but not necessarily the right content. They need to critically assess if they really have identified risks that could derail the company from achieving its objectives. Here are some of the top considerations for management when discussing risks:

- **Known risks**
  - Data breaches resulting in revenue leakages and information loss
  - Infringement of intellectual property rights
  - Disruption in the supply chain (third parties, suppliers and distributors)

- **Core operational risks**
  - Technology risks around deployment, cybersecurity and malfunctions
  - Ability to reduce costs and drive efficiencies
  - Operational capacity constraints (e.g. network, infrastructure and people) to support the digital transformation agenda

- **External environment**
  - Changing user behaviours and how services are consumed
  - Rapidly evolving regulatory landscape and accounting standards
  - Increased competition and disruption by non-traditional players

- **Emerging risks**
  - External emerging risks arising from the external environment
  - Successfully commercialising innovation and launching new products for revenue generation
  - Adaptability of business model to new platforms and forms of access
  - Risks from expanding operations globally

- **New risks**
  - Internally driven risks impacting day-to-day operations
  - Risks from changes required to implement the strategy
Top 10 internal audit considerations

The rapidly changing business environment highlighted by the top risks mentioned earlier puts the spotlight on how internal audit functions can proactively respond to the business’s assurance needs. Our ‘Top 10 considerations’ focuses on the critical role that internal audit can play in helping the business manage some of its leading risks in today’s dynamic environment. These are areas that heads of internal audit should be considering as they plan their internal audit activities for the coming year.

### Deploying new technology

**Drivers**
Rapid advances in technology have meant that companies have to continuously adapt to secure sources of revenue generation. At the same time, it is recognised that legacy systems are not sufficiently scalable, reliable, agile or responsive.

**Internal audit focus areas**
- System implementation reviews to assess consideration of strategy alignment, governance, project management, status reporting, tracking of business readiness and vendor management
- Processes by which management establishes a business case for cloud, performs due diligence for services provided, and monitors data and risks

### Third-party relationships

**Drivers**
Increased use of third parties to carry out vital functions exposes the company to a range of risks including security of sensitive data, management of outsourced relationships and control of cost, while ensuring that performance targets are met.

**Internal audit focus areas**
- Reviewing the third-party management programme, including vetting, due diligence and monitoring
- Evaluating contract management processes used to track third-party relationships
- Executing risk-based third-party reviews that include procedures tailored to address the specific risks a third party presents

### Revenue growth

**Drivers**
Global opportunities for growth remain top of the board agenda. This equates to a need to manage execution risk more effectively, particularly around revenue assurance, new business integration programmes, and oversight of global operations.

**Internal audit focus areas**
- Assisting in creating automated extract, transform and load (ETL) processes along with system-generated analytics/dashboards against specified risk criteria to allow for repeatable audits
- Developing data analytic-enabled audits focused on root cause analysis, business anomalies and trigger events to continuously review transactions

### Customer experience

**Drivers**
Increasing competitive advantage by improving customer loyalty, reducing customer service cost and avoiding reputational damage through better customer experience have all put the focus back on the customer.

**Internal audit focus areas**
- Evaluating how consistently customer service policies are applied across the company for each customer service channel
- Assessing if processes and controls designed to mitigate customer service risks are effective
- Reviewing metrics and indicators in place to evaluate customer service performance

### Internal audit focus areas

- **Drivers**
  - Revenue growth
  - Third-party relationships
  - Deploying new technology
  - Continuous auditing
  - Customer experience

© 2017 KPMG Advisory (Hong Kong) Limited, a Hong Kong limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in Hong Kong.
Cybersecurity

Drivers
In a world of constant connectivity, the consequences of data breaches such as legal fines, investigations, customer loss, remediation efforts and reputational damage to the organisation can be severe.

Internal audit focus areas
- Reviewing information management policies
- Reviewing the company’s ability to respond to new policies and regulations that may impact how the company stores, secures and uses data
- Reviewing processes and controls to collect, analyse, store and share personal information across the business

Data governance

Drivers
The explosion of data being captured and stored in big data platforms has introduced a new universe of risk into the business, including maintaining the accuracy and integrity of the data, and ensuring data security policies are established and followed.

Internal audit focus areas
- Reviewing and monitoring the compliance of third-party contracts including brand, technology, software rights and distributor/reseller agreements
- Reviewing IP processes across all elements of the IP life cycle including protection, management and enforcement

IP protection

Drivers
With business increasingly taking place through a network of separate entities (including joint ventures and alliances) using highly complex contracts, the management and protection of intellectual property (IP) remains of utmost importance.

Internal audit focus areas
- Real-time assessment of projects and control environment in high-risk areas such as project authorisation, scope changes, status reporting, fraud, contracting and vendor management
- Evaluating capital expenditure strategy with respect to expected outcomes, assumptions, new accounting standards and inherent risks

Compliance

Drivers
Increasing regulatory and accounting standard changes, aggressive enforcement, and management of multiple compliance activities across the company has meant that compliance activities can easily become complex and costly.

Internal audit focus areas
- Assessing the company’s overall compliance framework and determining if opportunities exist to more efficiently and effectively manage compliance across the organisation
- Auditing the design and operating effectiveness of processes and control activities intended to help the company comply with regulations/standards

Capital expenditure

Drivers
Companies have made large investments in capital projects to manage existing infrastructure. However, they continue to struggle with identifying new technologies that provide the most reward for the expenditure and have experienced inefficiencies in the effective use of funds.

Internal audit focus areas
- Top-down risk assessment around the cybersecurity framework using industry standards
- Reviewing existing processes and controls to assess how threats are considered, and the adequacy of security incident response systems
- Evaluating the extent to which third-party security providers are addressing current and emerging risk

Contact us

Our professionals combine industry knowledge with the technical capabilities and experience of our people across 152 countries to assist with performing internal audits (including data analytic and continuous monitoring roll-out), developing risk management systems and facilitating the identification of risks facing the business.

Paul McSheaffrey  
Partner, KPMG China  
E: paul.mcsheaffrey@kpmg.com

Alva Lee  
Partner, KPMG China  
E: alva.lee@kpmg.com

Karan Kumar  
Associate Director, KPMG China  
E: karan.kumar@kpmg.com