KPMG

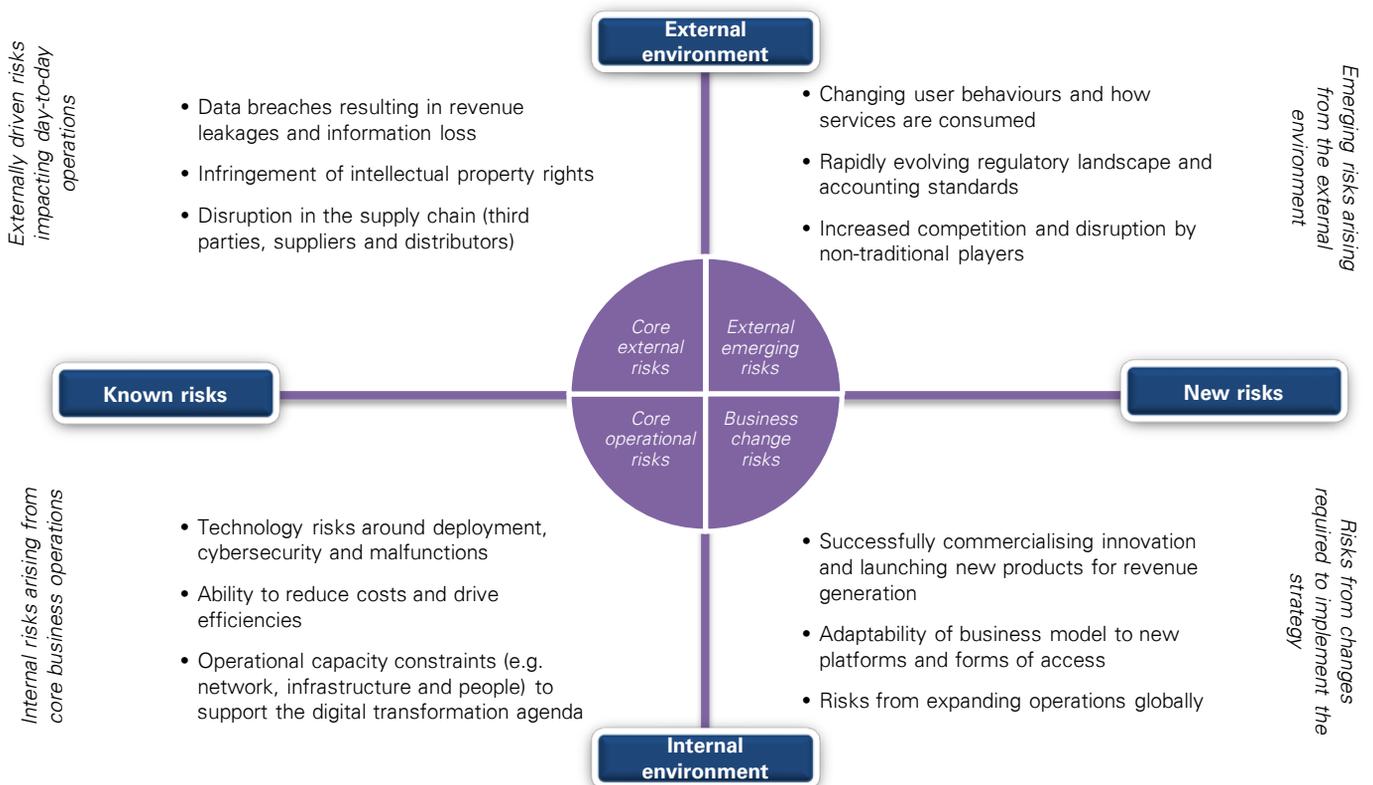# Disrupting internal audit functions in the TMT sector

kpmg.com/cn

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 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 in 2018 and 2019.

Top risks for 2018 and 2019

Some of the key areas of risk that heads of audit should be aware of include:

Externally driven risks impacting day-to-day operations

External environment

Emerging risks arising from the external environment

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

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

Core external risks

External emerging risks

Known risks

New risks

Core operational risks

Business change risks

Internal risks arising from core business operations

Risks from changes required to implement the strategy

- 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

- 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

Internal environment

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

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

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.

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

- Assessment of sales processes to ensure customers are billed completely and accurately
- Overall control environment across the global operations covering practices, processes and controls to comply with company requirements
- 'Post-mortem' reviews on new deals to assess the effectiveness of processes and controls

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

Continuous auditing

Drivers

Ever-evolving business models, new technologies and the changing ways in which customers consume services require that internal audit functions build real-time focus on emerging risks through expanded scope coverage and increasingly efficient audits using data analytics.

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

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

- 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

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 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

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

- 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

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

- 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

Contact us

Shanghai:

Li Fern Woo
Partner
Tel: +86 (21) 2212 2603
lifern.woo@kpmg.com

Grace Chen
Partner
Tel: +86 (21) 2212 2780
grace.xh.chen@kpmg.com

Joyce Ge
Partner
Tel: +86 (21) 2212 3295
joyce.ge@kpmg.com

Bryan Hu
Director
Tel: +86 (21) 2212 3686
bryan.hu@kpmg.com

Beijing:

Frank Mei
Partner
Tel: +86 (10) 8508 7188
frank.mei@kpmg.com

Jessica Xu
Partner
Tel: +86 (10) 8508 5952
jessica.xu@kpmg.com

Johnson Li
Partner
Tel: +86 (10) 8508 5975
johnson.li@kpmg.com

Vera Li
Director
Tel: +86 (21) 8508 5870
vd.li@kpmg.com

Haoyu Liu
Director
Tel: +86 10 8553 3343
haoyu.liu@kpmg.com

Hong Kong:

Alva Lee
Partner
Tel: +852 2143 8764
alva.lee@kpmg.com

Paul McSheaffrey
Partner
Tel: +852 2978 8236
paul.mcsheaffrey@kpmg.com

Jia Ning Song
Partner
Tel: +852 2978 8101
jianing.n.song@kpmg.com

Jeffrey Hau
Partner
Tel: +852 2685 7780
jeffrey.hau@kpmg.com

Susanne Steyn
Director
Tel: +852 2140 2317
susanne.steyn@kpmg.com

Karan Kumar
Director
Tel: +852 2847 5166
karan.kumar@kpmg.com

Guangzhou/Shenzhen:

Kelvin Leung
Partner
Tel: +86 755 2547 3338
kelvin.oc.leung@kpmg.com

Eric Chang
Partner
Tel: +86 20 3813 7088
eric.chang@kpmg.com

Joyce Xie
Director
Tel: +86 755 2547 1261
joyce.xie@kpmg.com

kpmg.com/cn