KPMG

Internal audit: Unlocking value for telecommunications companies

Top 10 internal audit considerations for telecommunications companies

July 2016

kpmg.com

This document outlines the critical role internal audit holds in helping telecommunications companies manage some of today's most important risk areas more effectively and unlock underlying value for the company in the process.

The 10 focus areas explore some of the leading risks telecommunications companies face as they strategize and make investments. KPMG LLP's (KPMG) selection of consideration areas is based on a number of inputs, including:

- Discussions with chief audit executives at telecommunications companies
- Insights from KPMG professionals who work with telecommunications companies
- Various KPMG-sponsored industry and technical accounting share forums
- KPMG survey data, including a recent study, Seeking value through Internal Audit, in which KPMG and Forbes surveyed more than 400 chief financial officers and audit committee chairs to identify the insights internal audit functions are providing, as well as opportunities where internal audit organizations can improve.

Note: Every telecommunications company is unique and it is important that internal audit rely on a company-specific analysis of its risks in developing its internal audit focus areas.

Top 10 internal audit considerations for telecommunications companies

1. Cybersecurity
2. Capital expenditures
3. Data governance
4. Customer experience
5. Network data integrity
6. Increasing demand
7. Data analytics and continuous auditing
8. Third-party relationships
9. Accounting change
10. Regulatory change

1. Cybersecurity

Drivers:

- Avoiding costly consequences of data breaches, such as investigations, legal fines, coverage of customer losses, remediation efforts, loss of executive and midlevel time and focus, and potential loss of customers and business
- Averting reputational damage to the organization, especially with regard to lost customer data
- Mitigating exposure to new kinds of risks related to new services and more and more connected devices
- Preventing loss of intellectual property, capital, and other privileged company information

In today's world of constant connectivity, cybersecurity has emerged as a key focus area for telecommunications companies. As telecom networks have become an integral part of our daily lives, they have changed the way we communicate and interact with others, work, and relax. Further, telecom networks are a critical component of our national infrastructure, similar in many ways to our system of roads and highways, and are an important contributor to economic growth.

Several factors continue to drive the increased attention to cybersecurity issues, including rapid shifts in technology and the threat landscape, more stringent and diverse regulatory environments, social change, and changes in corporate culture.

The capabilities and techniques used by hackers evolve continuously, especially in targeting specific information or individuals. New methods are constantly being developed by increasingly sophisticated and well-funded hackers—including organized crime, nation states, hacktivists, and insiders—who can target companies not only directly but also through social engineering, phishing scams, and connections with key suppliers and technology partners.

The consequences of lapses in security can be disastrous as an organization's bottom line and reputation are impacted. It is critical for technology companies to remain vigilant and up-to-date on emerging threats and protection criteria.

Internal audit can execute technical and process-driven assessments to identify and evaluate cybersecurity risks, and offers strategies and recommendations to help mitigate the identified risks.

Example focus areas for internal audit:

- Performing a top-down risk assessment around the company's cybersecurity framework using industry standards as a guide and providing recommendations for process improvements
- Reviewing existing processes and controls to help ensure they consider the threats posed in the constantly evolving environment
- Reviewing the alignment of the organization's cybersecurity framework with regulatory expectations
- Assessing implementation of revised technology security models, such as multilayered defenses, enhanced detection methods, and encryption of data leaving the network
- Evaluating the organization's security incident response and communications plans
- Assessing third-party security providers to evaluate the extent to which they are addressing current and emerging risks completely and sufficiently
- Determining if management has performed a maturity assessment of cyber capabilities on a site-by-site basis or at a company level

2. Capital expenditures

Drivers:

- Rapidly evolving network and service delivery technologies
- Upgrading, maintaining, or expanding existing networks and supporting infrastructure, such as converting to IP-based edge and core network technologies, acquiring advanced wireless spectrum, or implementing cloud-based software-defined networking capabilities
  - Increasing demand for telecommunications services resulting from increasing use of mobile and connected devices
  - Changing capital expenditure strategies
  - Implementing new lease accounting standards

Telecommunications companies have always struggled to identify new technologies that provide the most reward for the associated capital expenditure. Many have experienced inefficiencies in the effective use of capital expenditures, while global demand for telecommunications services continues to drive the need for increased capacity and speed of wireless data networks.

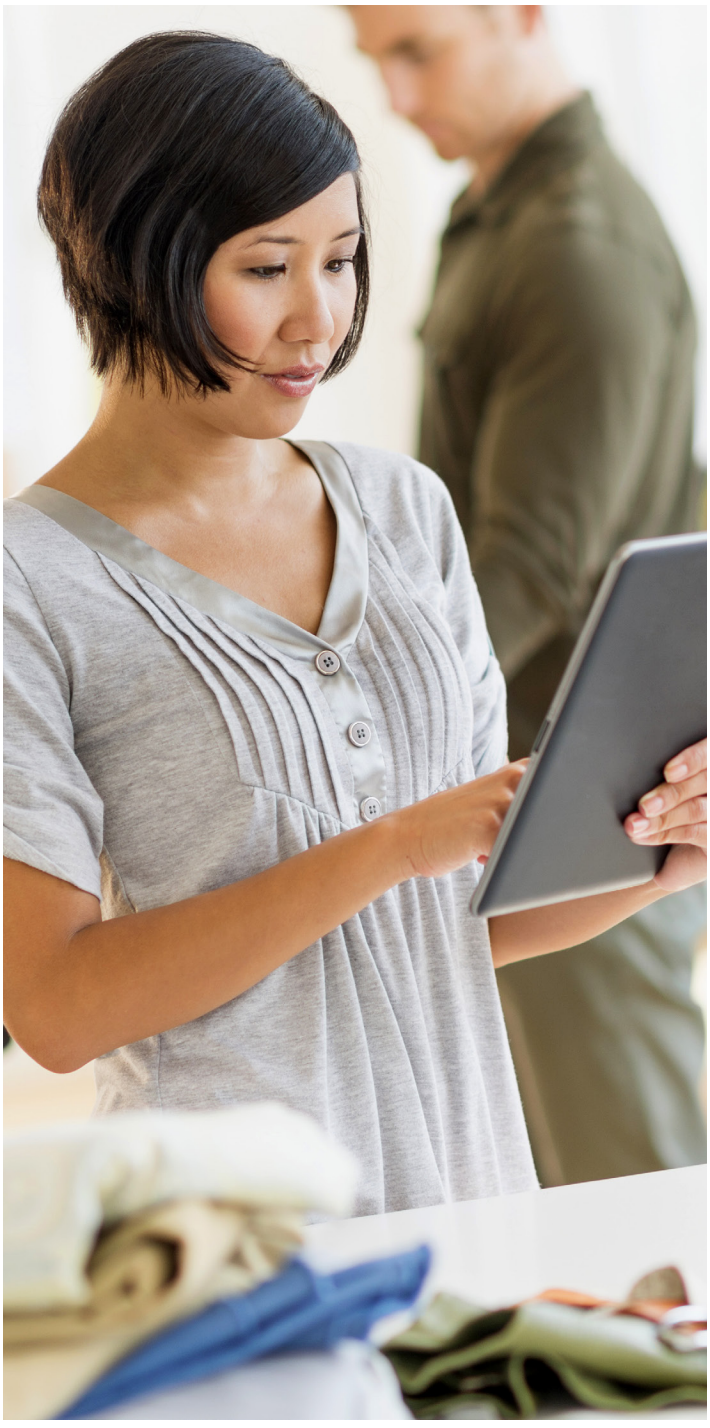
Responding to this demand, telecommunications companies have spent billions of dollars on capital projects over the last several years. Additionally, many are implementing capital expenditure strategies that employ, for example, greater use of leases as a way to mitigate risks or to manage cash flow. These aspects present unique challenges for executives responsible for strategic alignment, accountability, financing, and a suitable control environment.

Example focus areas for internal audit:

- Performing a review of planned capital projects to assess management's consideration of strategic alignment, project planning, and authorization
- Evaluating the vendor authorization and procurement process to ensure compliance with policies
- Performing real-time assessments of individual capital expenditure projects to identify potential issues with project management, status reporting, and vendor compliance with contract terms and provisions
- Assessing the policies and control environment of key high-risk areas, such as project authorization, contracting, scope changes, and fraud
- Evaluating capital expenditure strategy with respect to expected outcomes, assumptions, new accounting standards, and risks inherent with the strategy
- Performing lookback reviews of capital projects, including reviewing assumptions and outcomes

KPMG

3. Data governance



Drivers:

- Validating and maintaining the accuracy, integrity, and versioning of a company's big data
- Ensuring proper data security policies are established and being followed
- Increasing usability and metadata comprehension by business owners
- Operationalizing metadata to make it actionable

There is an explosion of data being captured and stored in big data platforms. Leading organizations across all industries are leveraging the power of big data technologies to capture, merge, and analyze internal and external, structured and unstructured, and transactional and historical data to change the way they run their businesses, and in some cases, create new businesses. The benefits are not without risks. For example, data must be secured and certain types of data, such as customer proprietary network information (CPNI) and other personal identifiable information (PII), are specifically regulated. Increasingly, companies are required to obtain customer consent to use their data or disclose to customers how their data will be used and shared. Internal audit plays a key role in ensuring big data does not cause big problems.

Example focus areas for internal audit:

- Assisting in the formation or review of data governance policies and processes to increase the accuracy and integrity of a company's metadata
- Documenting the data model and points of control to identify security gaps (e.g., understanding what data is collected, where it is stored, how it is used, and who has access)
- Helping design or review information management policies that include designing, organizing, retrieving, and distributing information in the most efficient manner
- Reviewing the company's ability to appropriately respond to new policies and emerging regulations that may impact how the company stores, secures, and uses data

KPMG

4. Customer experience

Drivers:

- Increasing an organization's competitive advantage through better customer experiences, for example, by providing seamless service experiences to customers who are increasingly demanding quick resolution through channels of their choice, including social media
- Avoiding reputational damage to the organization resulting from poor customer service
- Assessing customer behaviors and usage patterns to introduce relevant products and services in a timely manner, and enable product innovations and creativity, thereby resulting in increased customer loyalty, gross additions, and profitability
- Reducing customer service costs and increasing process efficiencies through improving service delivery processes or leveraging technology

The topic of customer service and overall customer risk has traditionally been limited to the completeness and accuracy of billing, discount and rebate processing, call center cost reduction, and customer retention. Although these topics continue to be important, there is a growing need to make a paradigm shift to a more strategic and tactical approach. As a result, topics driving customer strategy are increasingly focused on leveraging customer behavior prediction through data analytics, enhancing value and efficiency in sales and marketing efforts as they directly target the most valued stakeholder of the organization—the customer. Correspondingly, investments in tools and processes to support this strategy are gaining more attention.

Internal audit, with their overall organizational knowledge and influence, can support this initiative and should be perceived as a valued business advisor and contributor. Customer-focused processes, policies, and initiatives should come under the internal audit lens not just from a risk, controls, and compliance perspective but also from a potential process improvement and enhancement standpoint.

Example focus areas for internal audit:

- Reviewing the processes used by the organization to identify, analyze, and manage customer service risks
- Comparing existing customer service processes, policies, and tools with leading industry trends and recommending potential changes and enhancements
- Evaluating if customer service policies and procedures (e.g., roles, responsibilities, metrics, and key performance indicators) are current and consistently applied across the organization for each customer service channel
- Assessing if processes and controls designed to mitigate customer service risks are designed and operating effectively
- Reviewing the key performance indicators and metrics used to evaluate customer service performance, including more general indicators, such as net promoter scores
- Evaluating the organization's ability to leverage data analytics to predict customer behavior and develop relevant responses
- Evaluating the efficiency of the organization's processes and tools used to capture social media trends and other information available on emerging platforms

5. Network data integrity

Drivers:

- Reducing end-user billing errors and avoiding unnecessary expenses related to unused or underutilized leased access
- Large or growing order backlog resulting from difficulties identifying network assets that are available for use (or reuse) when provisioning new services or an inability to automate all or parts of the provisioning work flow
- Difficulties correlating or isolating network troubles resulting in long repair times (or mean time to repair)
- Decreasing the percentage of service orders with errors or that require rework

In the highly competitive telecommunications industry, service quality and reliability can be an important differentiator. A well-run network can help improve the customer experience, reduce churn, and lower operational costs. An important component of reliably and efficiently operating a telecommunications network is a complete and accurate network and service inventory. However, maintaining network inventory data integrity is a constant challenge driven by many factors, including:

- Maintaining a subscriber base of thousands or millions of customers
- A complex catalog of new and legacy services
- Mergers and acquisitions of companies with different technologies and operational practices
- Service provisioning (and deprovisioning) processes that may not be well-controlled.

Leading telecommunications companies recognize the importance of network data integrity and work to ensure that robust operational processes and controls exist to help ensure network data integrity is maintained, or where needed, improved. Network data is complex, and pinpointing network data integrity issues can be challenging. Telecommunications technology and operations subject-matter professionals can also be an invaluable resource when assessing network data integrity.

Example focus areas for internal audit:

- Determine if a sample of active network services are billing to the customer completely and accurately; if possible, select the sample by inspecting active services directly in the network (e.g., through an operational support system or by physically inspecting network equipment); If the service is not billing, determine if it should be or if the underlying equipment can be redeployed
- For a sample or leased or "off-net" circuits (e.g., from carrier access bills), determine if each is accurately represented in the network inventory, and where applicable, determine if the leased circuit can be matched to its corresponding revenue-generating service
- Inspect network incident and outage reports and related repair activities (e.g., in service tickets); through inspection or inquiry of network operations personnel, determine if repairs were hindered by inaccurate or incomplete network inventory information
- Assess the company's ability to meet service delivery dates, and if necessary, determine the root cause of service delivery delays
- Inspect the complete process from sales order entry to service delivery. Determine the percentage of sales orders requiring rework, and if opportunities exist, automate sales order processing (to decrease service delivery cycle time and reduce errors)

KPMG

6. Increasing demand

Drivers:

- Increasing use of mobile and connected devices
- Avoiding disruptions caused by high demand or high traffic volume, especially during peak hours
- Protecting the brand perception for network quality and reliability, or perhaps improving those perceptions
- Changing technology and the ability to obtain and deploy capital in order to execute against the company's strategy

Ever-evolving technology and increasing demand for telecommunications services has become the norm. In retrospect, even in the days of point-to-point wireline communications, the industry has been defined by its unique mix of utility and technological innovation. Few would argue the contributions to economic growth made possible by access to an advanced, affordable communications infrastructure. Today, this trend continues, albeit at a much faster pace, as recent technological advances in both telecommunications technology and "connected" devices are fueling greater demand for faster, reliable, and always on access. This trend is expected to continue in today's rapidly evolving innovation-focused marketplace.

Example focus areas for internal audit:

- Assessing network operations risks by evaluating the impact of increased demand on network management practices. This can include performing analytical procedures to evaluate network reliability while also considering network management practices to manage peak demand
- Evaluating the processes management uses to forecast demand and correspondingly provide the required capital to meet forecasted demand or needed to implement the company's strategy
- Assessing technology-related risks, for example, by evaluating capital investments and determining if these investments make sense in light of current technological advances (e.g., acceptance by standards-setting bodies or comparing the company's plans to deploy a particular technology with others' regional or global implementations or plans to implement)
- Note that partnering with subject-matter experts can be especially helpful when executing internal audit projects in any of these areas

7. Data analytics and continuous auditing

Drivers:

- Robustly and timely addressing existing and emerging risks, for example related to evolving business models, new technology, and the changing ways in which customers consume telecommunications services (e.g., through different mobile applications or connected devices)
  - Creating value by leveraging advanced "big data" tools and techniques implemented by management to quickly adapt to rapidly evolving business demands
  - Improving internal audit quality and efficiency while reducing costs and improving risk coverage

Data analytics have helped improve the way internal audit departments assess and monitor risks, especially in terms of enabling expanded risk coverage and audit scope and improving testing precision. Continuous auditing can help internal audit departments simplify and improve the audit process, resulting in higher quality audits and increased value to the business through the use of repeatable and sustainable data analytics that can provide for more precise control evaluation. Additionally, given that audit committees and stakeholders are asking internal audit to do more for less, these techniques can allow for more controls to be evaluated, resulting in greater coverage.

While internal audit departments can realize significant benefits by employing data analytics and continuous auditing techniques, those responsible for operations, compliance, and financial reporting have also generally increased their use of data analytics and continuous monitoring techniques in executing their responsibilities. Internal audit departments can often leverage these platforms or assist in a consulting role to help improve processes and controls leveraging these capabilities. Although Internal Audit must maintain an adequate degree of separation from management responsibilities, opportunities exist to work with management to expand the use of data analytics and continuous monitoring and auditing techniques.

Example focus areas for internal audit:

- Assisting in creating automated extract, transform, and load (ETL) processes, along with repeatable and sustainable analytics and dashboards enabling auditing or monitoring against specified risk criteria by internal audit or business management
- Assessing the alignment of the strategic goals and objectives of the company to risk management practices while providing a mechanism to monitor and prioritize strategic objectives and risks on a continuous basis
- Developing data analytics enabled audit programs designed to verify the underlying data analysis and reporting of risk at the business level
- Performing automated auditing focused on root cause analysis and management's responses to risks, including business anomalies and trigger events
- Recommending consistent use of analytics, including descriptive, diagnostic, predictive, and prescriptive elements

KPMG

8. Third-party relationships

Drivers:

- Increasing the use of third parties to carry out vital business functions
- Securing sensitive data that may be stored and utilized by third-party vendors
- Mitigating risks unique to managing outsourcing relationships, such as controlling costs and ensuring performance obligations are met
- Cost cutting measures often focused on outsourcing noncore business functions

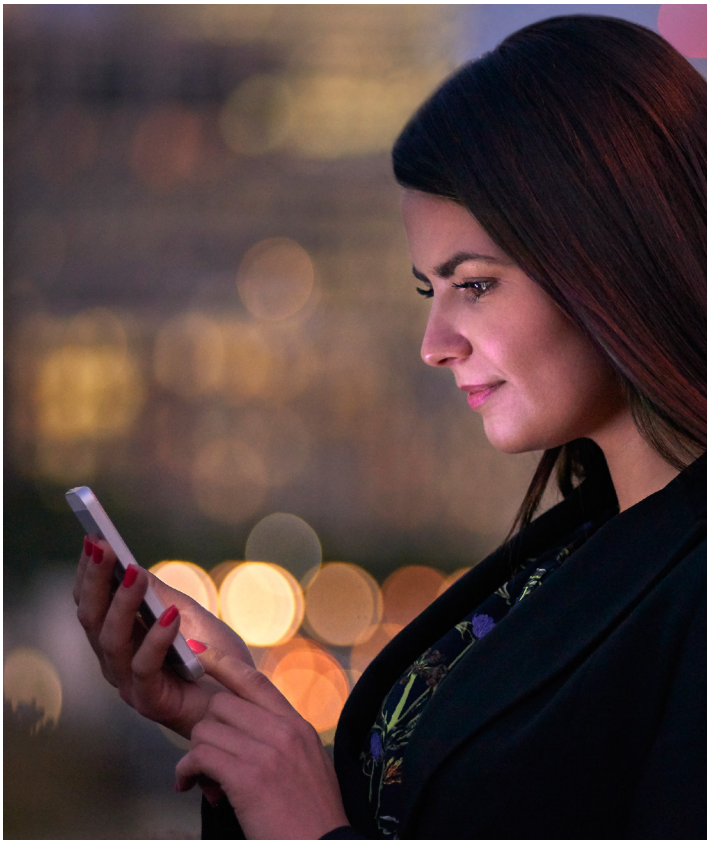
Telecommunications companies leverage third parties for a variety of services, such as billing, network operations, information technology support, data center hosting, and customer service. Outsourcing frees up organizational resources to focus on core competencies and can help reduce costs.

While third parties provide valuable services, they can expose an organization to financial, compliance, and operational risks. These risks can be extensive, including revenue loss or penalties, data privacy breaches, service disruption, bribery, and corruption risk, any of which may damage the company's reputation. Organizations have the ability to outsource a variety of tasks; however, they remain accountable for these outsourced activities.

An effective third-party management program, such as one that incorporates third party risk assessment, due diligence, and ongoing monitoring, can help companies manage their exposure to these risks.

Example focus areas for internal audit:

- Evaluating the methodology the organization uses to identify third parties, including segmentation and classification, and the risks associated with them
- Providing insight and feedback on the organization's third-party management program, including vetting, due diligence, and monitoring
- Executing risk-based third-party reviews that include procedures tailored to address the specific risks a third-party presents
- Investigating anomalies identified as a result of the organization's third-party vetting process



9. Accounting change

Drivers:

- Implementing new accounting policies, processes, controls, and supporting IT infrastructure to effectively meet upcoming implementation deadlines related to new accounting standards, such as the new revenue recognition and leasing standards issued by the Financial Accounting Standards Board (FASB)
- Considering the company's revenue-generating activities, the corresponding performance obligations, and the implications of the new standard to accounting for these activities
- Identifying and assessing the full population of leases that may be impacted by new leasing standards
- Considering potential impacts to downstream processes that rely on inputs that may change due to new accounting standards, for example financial reporting, debt covenants, regulatory fees, and taxes

The Financial Accounting Standards Board (FASB) has issued a large number of revised, updated, or new standards that have to be implemented within relatively short time periods. Due to the magnitude and complexity of changes involved, this has, at least in some industries, almost the same impact as first-time adoption. In this paper, we focus on two significant account changes—revenue recognition and lease accounting—that have broad implications for telecommunications companies.

Revenue recognition – Public companies should apply the new revenue recognition standard to annual reporting periods beginning after December 15, 2017. Nonpublic companies should apply the new revenue standard to annual reporting periods beginning after December 15, 2018. The new revenue recognition standard may require telecommunications entities to change their accounting for certain types of transactions. Implementation will be challenging for many telecommunications companies because of the nature of the company's products and service (and related service bundles), the variety of plans offered, and the frequency with which customers modify their plans.

Lease accounting – Public companies should apply the new leasing standard for interim and annual periods beginning after December 15, 2018. Private companies should comply for annual periods beginning after December 15, 2019 and for interim periods beginning a year later. Early adoption is permitted. The FASB's new lease accounting standard requires organizations to recognize most leases, on-balance sheet, which increases their reported assets and liabilities. Implementation will be challenging for many telecommunications companies, as they collect leasing data across multiple disparate data sources in order to assess impacts to least accounting, as well as impacts to IT systems and processes, and people.

Example focus areas for internal audit:

- Performing readiness assessments to identify potential gaps in the company's future ability to report under the new standards
- Assessing capabilities in current accounting and information systems to meet the requirements of the new standards and support downstream systems and business processes
- Perform postimplementation reviews to help ensure enhancements made to processes and technologies will adequately meet expectations of the new standards
- Internal control evaluations over new or updated controls implemented to help ensure compliance with the new standards

10. Regulatory change

Drivers:

- Changing the regulatory landscape, including new or evolving direct telecommunications regulation (e.g., rules promulgated by the Federal Communications Commission (FCC) or state commissions) and other regulations that a telecommunications company may need to comply with, depending on various business activities (e.g., Health Insurance Portability and Accountability Act or Federal Acquisition Requirements)
- Increasing government enforcement
- Managing multiple compliance activities across the company

There are many drivers of the regulatory changes impacting telecommunications companies. For example, changing technologies and competition are driving new regulations around net neutrality and intercarrier compensation. The ways in which consumers utilize telecommunications services are driving the need for new privacy rules. Specific company activities or transactions may require the company to comply with additional regulations. Therefore, a company's compliance activities can become complex and costly; especially if compliance activities are fragmented. Adding additional concern, government enforcement efforts have become increasing aggressive.

Internal auditors can assist with evaluating all five components of a company's internal control to help ensure compliance objectives are achieved. Internal auditors are also well-positioned to assess the efficiency and effectiveness of the company's compliance frameworks and processes to help minimize compliance costs.

Example focus areas for internal audit:

- Assessing any of the five internal control components as it relates to compliance objectives, such as the following:
  - Evaluating the company's control environment, including compliance programs, and assessing the company's "tone-at-the-top" and whistle-blower programs
  - Auditing the design and operating effectiveness of processes and control activities intended to help the company comply with specific rules or regulations
- Assessing the company's overall compliance framework or frameworks and determining if opportunities exist to more efficiently and effectively manage compliance across the organization
- Assisting with the internal discovery and remediation of actual or potential noncompliance incidents

KPMG

About the authors

Paul Wissmann
National Sector Leader,
Media & Telecom Practice
Los Angeles, CA

Paul Wissmann is the National Sector Leader of KPMG's Media and Telecommunications practice with 30 years of experience at KPMG. Paul's career has been focused on providing services to media, telecommunications, information and entertainment clients. He has provided both audit and advisory services. Paul is both a U.S. and international resource to the firm on matters related to the entertainment and telecommunications industry including business and accounting issues. He has written and presented on many business issues currently experienced by the media and telecommunications business, including the transformative changes being experienced within these industries. He has consulted with companies regarding the implications of these changes to their business models and potential acquisitions.

Shruti K Shah
Managing Director, Internal Audit Leader
for Telecommunications
Short Hills, NJ

Shruti Shah is a Managing Director in KPMG's Advisory Services Practice with over 20 years experience and currently serves as KPMG's Internal Audit Lead for Telecommunications. In this role she serves some of the industry leading Telecom companies to assist as an organizational change driver involved in various corporate transformation initiatives to improve performance and reduce risk and compliance exposures. She has led large scale projects that cover the following topics: Internal Audit, Risk Assessments, Compliance Transformation, Enterprise Risk Management, Policy, Process and Technology, Governance, Project/ Financial Management and Talent Management. A significant portion of Shruti's career has been involved with assisting clients with the coordination and execution of large scale International Projects.

Alfie Mahmoud
Managing Director
Advisory Services
Kansas City, MS

Alfie A. Mahmoud is a Managing Director in KPMG's advisory practice. He has over 20 years of combined industry and consulting experience, including 15 years providing professional services primarily to domestic and international telecommunications industry clients since joining KPMG in 1999.

With a background in both business and engineering, Alfie is uniquely qualified and adept at recognizing how telecommunications technologies and operations impact downstream processes and controls in areas such as finance and accounting, billing, revenue and cost assurance, regulatory compliance, and financial reporting. He also has extensive experience helping clients integrate acquired businesses, and manage and settle billing disputes, including providing expert testimony. Alfie delivers these services through several client channels including finance and accounting, operations, internal audit, and under the direction of counsel. In addition to his professional practice, Alfie helps develop and deliver industry training courses, as well as courses in risk management, control evaluation and process improvement.

KPMG

Contributors

We acknowledge the contribution of the following individuals who assisted in the development of this publication:

Carrie Erwin
Director, Advisory

Hemendra Upadhyay
Director Advisory

How KPMG Can Help

An experienced team. A global network. KPMG's Internal Audit, Risk and Compliance professionals combine industry knowledge with technical experience to provide insights that help communications industry leaders take advantage of existing and emerging opportunities and proactively manage business challenges.

KPMG's Advisory professionals combine technical, market and business skills that allow them to deliver objective advice and guidance that helps our clients grow their businesses, improve their performance, and manage risk more effectively.

Our professionals have extensive experience working with global communications companies ranging from the world's largest carriers to alternative providers and MVNO startups. We go beyond today's challenges to anticipate the potential long- and short- term consequences of new technologies, regulatory changes and evolving customer demands. With a worldwide presence, KPMG continues to build on our member firms' successes thanks to our clear vision, maintained values, and our people in 155 countries. We have the knowledge and experience to navigate the global landscape.

Contact us

Paul Wissmann
National Sector Leader,
Media & Telecommunications
213-955-8518
pwissmann@kpmg.com

Richard Hanley
U.S. National Advisory Leader,
Technology, Media & Telecommunications
408-367-7600
rhanley@kpmg.com

Shruti Shah
Managing Director, Internal Audit Leader for
Telecommunications
973-912-6316
skshah@kpmg.com

Alfie Mahmoud
Managing Director
913-907-4029
amahmoud@kpmg.com

kpmg.com/socialmedia