KPMG Internal Audit: Top 10 key risks in 2016

Banking and Capital Markets

kpmg.com

KPMG
cutting through complexity

Six years after the financial crisis, internal auditors at banks and capital markets firms continue to face increased pressure internally and externally. Internally, the pressure comes from the board of directors, executive management, and business unit stakeholders. Externally, it originates from regulatory authorities—the Securities and Exchange Commission (SEC), the Federal Reserve Board, Office of the Comptroller of the Currency (OCC), Consumer Financial Protection Bureau (CFPB), Financial Industry Regulatory Authority (FINRA), and investors.

Political, regulatory, and legal authorities and the media continue to highlight shortcomings in the industry, and regulatory agencies are growing increasingly impatient with failures to invest adequate resources to address their concerns. Internal auditors are considered part of the solution, and they must continue to:

- Improve the risk identification and assessment process
- Take a forward-looking and proactive approach to internal audits/reviews
- Effectively challenge the first and second lines of defense
- Identify relevant issues and provide value-add recommendations to business unit stakeholders—all while maintaining the independence and objectivity expected of an organization's third line of defense.

This article highlights what should be top of mind for chief auditors and their teams during the upcoming year. It is based on our conversations with chief audit executives at banks and capital markets firms and internal audit executives at our share forums, as well as insights from KPMG partners and professionals who work in the industry.

The result is our "Top 10 in 2016"—key considerations that internal auditors at banks and capital markets firms should evaluate as part of their overall strategy, risk assessment, and internal audit plan.

1	Increased regulatory expectations
2	Culture and conduct
3	Regulatory reporting
4	Stress testing
5	Model risk management
6	Cybersecurity
7	Third-party relationships/vendor management
8	Continuous risk assessment
9	Use of data analytics and continuous auditing
10	Internal audit talent recruitment and retention

1 Increased regulatory expectations

Drivers:

- Continuing the identification and settlement of legacy financial crisis issues
- Perception of the industry by the media and public
- Agendas of various regulatory agencies
- Benchmarking of entire industry against those who are best in class
- Meeting the requirements of FRB[1] : Supervisory Letter SR13-1 Supplemental Policy Statement on the internal audit Function and Its Outsourcing (SR13-1)

Large banks and capital markets firms continue to fall under the purview of multiple global and national regulators and are challenged with meeting the ever-increasing demands of these regulators, who may have common or even conflicting agendas/interests/viewpoints. Legislative bodies have empowered regulators to enact tens of thousands of pages of new rules and regulations impacting the entire financial services industry. In addition, many of these regulations have yet to be fully implemented and remain in the pipeline for years to come.

Banks and capital markets firms must react swiftly and adjust their business models appropriately to remain competitive within the marketplace and compliant with the rules and regulations. An additional challenge organizations encounter is that regulators have a line of sight into the control environments, risk assessments, systems, etc., throughout the industry and are able to form a horizontal view into those organizations with best-in-class operations. As a result, the regulators' perspective of best practices is constantly evolving, causing management, risk functions, and internal audit to stay current on the changing regulatory landscape to keep pace with the expectations of their regulators.

Internal auditors may bridge the gap by serving as trusted advisers to management and by providing insights and guidance about where regulators may focus their efforts. internal audit also plays an important role in the tracking of issues and monitoring of remediation within the organization. The Board of Governors of the Federal Reserve System also implemented SR13-1, which applies to supervised institutions with greater than $10 billion in total consolidated assets. SR 13-1 provides internal audit functions with specific guidance and expectations in relation to the following areas:

- Corporate governance considerations
- The adequacy of the internal audit function's processes
- Internal audit performance and monitoring process
- Internal audit outsourcing arrangements.

Internal auditors must remain actively engaged within industry associations to allow for knowledge sharing, as well as to network to identify how peers are addressing such challenges and reacting to and perceiving regulators' expectations.

[1] FRB: Board of Governors of the Federal Reserve System

How Internal Audit can help:

- Perform readiness assessments on behalf of business lines to identify deficiencies and performance improvement opportunities prior to the formal implementation of rules/regulations
- Perform quality assessment reviews against the standards established by SR13-1
- Identify rules and regulations that are applicable to the organization's business model
- Pilot assurance programs/independent testing over areas where such may be necessary on a go-forward basis
- Provide an enterprise-wide view on the adequacy of the risk management and compliance function and how well the organization is staying current on the changing regulatory environment across all relevant jurisdictions
- Involve regulatory subject matter professionals through training and hiring practices and/or cosource arrangements to ensure that audit teams are effectively challenging the first and second lines of defense as they relate to help applicable laws and regulations
- Assess whether the policies and procedures and the control environment are kept current with regards to changing regulatory requirements

2 Culture and conduct

Drivers:

- Impact of culture and conduct on the performance of the business and achievement of business objectives
- Increase satisfaction and trust among customers, regulators, employees, and external stakeholders
- Foundational element in support of the organization's risk strategy and risk appetite
- The need for internal audit to provide a view of the adequacy of the risk management function across the organization

Political, regulatory, and legal authorities and the media continue to highlight deficiencies and issues concerning culture and conduct within banks and capital markets firms. These have resulted in financial losses in the billions of dollars and also exposed organizations to nonfinancial risk when their conduct and values do not in align with societal norms and expectations.

The tone at the top guides the culture and conduct of an organization, and executive management needs to continually assess whether its objectives and values are representative of a good culture. In addition, executive management must ensure employees exhibit its core values and expectations during internal and external interactions.

Executive and senior management may implement entity-level "instruments" through charters, policy and procedure manuals, risk and control matrices, etc., to guide employee behavior and facilitate achievement of the organization's objectives. Employees should be incentivized, through financial and nonfinancial compensation, to display behaviors expected of them and be held accountable when in conflict. While culture and conduct is usually viewed as intangible, there are various methods that organizations may leverage to measure their current state and progress, including surveys, interviews, roundtables, and benchmarks against peers and the industry.

How Internal Audit can help:

- Survey employees to determine whether responses align with the goals and objectives defined by the board of directors and executive management
- Through qualitative and quantitative analysis, benchmark the organization's culture and conduct against industry norms and identify needed improvements
- Construct a road map for executive management to strengthen the organization's culture and conduct
- Identify common "cultural" themes across the audit universe that could highlight issues associated with culture and conduct
- Perform a root-cause analysis of findings for potential linkage to culture and conduct

3 Regulatory reporting

Drivers:

- Potential disconnect between personnel knowledgeable about complex rules, regulations, and reporting requirements versus those responsible for the organization's end-to-end processes
- Integration of legacy systems and inconsistent datasets resulting from post-crisis, large-scale mergers and acquisitions
- Data integrity issues (e.g., completeness and accuracy) identified by regulators

Historically, regulators focused on the reporting of quantitative information; however, since the financial crisis, there is greater emphasis on the reporting of qualitative information through exercises such as stress testing and scenario analyses. Banks and capital markets firms face a number of challenges to producing core regulatory reports, including:

- Significant amount of manual reconciliations
- Data integrity issues
- Legacy system limitations
- Analytical challenges
- Resource and time constraints
- Governance weaknesses.

Regulators appear to be growing increasingly impatient with the industry's lack of progress in addressing these challenges. The industry needs to work towards producing a holistic approach to data governance.

How Internal Audit can help:

- Validate the integrity of data quality and processes on an ongoing basis through regular review and off-cycle testing
- Map end-to-end processes (e.g., finance, operations, etc.) impacting regulatory reporting and identify areas of weakness, process improvements, and the overarching control environment
- Serve as a participant on internal governance committees to proactively identify the impact that changes to systems, business lines, etc., may have on regulatory reporting
- Assess the awareness and knowledge of regulatory reporting for key personnel responsible for functions which may impact the regulatory reporting process and identify those who may require additional knowledge, training, etc.

4 Stress testing

Drivers:

- Coverage and focus on testing results by external stakeholders (e.g., regulators, investors)
- Expectations for design, implementation, and maintenance of a robust data collection process to support periodic and ad hoc stress testing
- Integration between stress testing and business-as-usual processes (e.g., budgeting)

As a result of the financial crisis, Congress enacted the Dodd-Frank Wall Street Reform and Consumer Protection Act, which implemented annual stress tests over bank holding companies (BHCs) with $50 billion or more in total consolidated assets. These annual stress tests are overseen by the Federal Reserve Board[2] (the Board) and evaluate the adequacy of BHC capital based on a number of factors, including planned capital actions, firmwide risk identification, risk measurement, risk-management practices, and strength of internal controls. The purpose of these stress tests is to identify the impact of and mitigate potential financial instability within the overall economy that may result from a BHC failure.

Over the years, the Board has shifted between various themes and areas of focus, and its expectations have continued to increase for stress testing programs and scenarios that banks have in place. Banks continue to be challenged throughout the annual stress testing exercise as regulators continually raise the bar for compliance. Internal audit may serve in an integral role throughout the process by assisting business units through various means, including:

- Reviewing models the bank relies on to facilitate the process
- Identifying and testing relevant controls, reconciliations, etc., to provide assurance to management that processes are operating effectively
- Reviewing prior-year submissions and identifying potential areas of weakness and process improvement opportunities.

How Internal Audit can help:

- Implement an independent review of the inputs, outputs, and reporting results of stress tests within the internal audit plan
- Serve as a participant on relevant governance committees and provide insights to the annual stress testing exercise
- Review and inquire of management how the inputs and results of the annual stress tests are factored into business-as-usual processes
- Assess the adequacy of the organization's data gathering capabilities, data quality, and extent to which automation is leveraged to maximize efficiency and flexibility
- Evaluate whether the organization's risk management and internal control infrastructure is keeping pace with changes to the risk profile, external risk landscape, and industry practices

[2] Board of Governors of the Federal Reserve System

5 Model risk management

Drivers:

- Regulators request and requirement to maintain adequate supporting documentation for look-backs and validation exercises
- Decisions based on incorrect or misused model outputs and reports may lead to financial loss, poor business and strategic decision making, or damage to reputation
- Limited personnel with technical competence and knowledge of a model's assumptions, thus restricting the ability to effectively challenge model developers

Guidance issued by the OCC and the Federal Reserve Board through OCC Bulletin 2011-12[3] and Fed SR 11-7[4] establishes three elements that create an appropriate model risk management framework: (1) sound development, implementation, and use of models; (2) robust model validation procedures, discipline monitoring, and back-testing; and (3) governance and control, including board and senior management oversight, policies and procedures, board model risk tolerance, controls and compliance, model inventory, and appropriate incentive and organizational structure.

Internal auditors may provide assurance over the aforementioned through the following: (1) evaluation of the conceptual soundness of models, including reviewing developmental evidence; (2) performing ongoing monitoring, including process verification and benchmarking; and (3) analyzing outcomes, including back-testing.

Effective model risk management continues to be an area of focus by internal stakeholders and regulators, as a result of the importance and impact that financial models have on everyday decision making within organizations. Regulators expect internal auditors to play a significant role in model validation programs and be able to provide effective challenge of models. Additionally, model validators need to remain independent of those individuals responsible for developing, owning, and using the model.

How Internal Audit can help:

- Perform an assessment of the overall adequacy of the organization's model development and change management life cycle policies, procedures, and control environment
- Inventory the models utilized by the business and assess whether there is appropriate ownership and governance over each model, as well as, segregation of duties between those developing and using the financial model
- Select a subset of models and assess whether the organization's model development and change management life-cycle is appropriately followed in practice
- Assess the range of scenarios that models are reviewed against and assess the overall adequacy (ensure both normal and black swan scenarios are included)
- Benchmark the organization's current model risk management processes against leading practices and industry standards

[3] http://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf
[4] http://www.federalreserve.gov/bankinforeg/srletters/sr1107.htm

6 Cybersecurity

Drivers:

- Avoiding costly consequences—investigations, legal fines, coverage of losses and potential loss of customers, remediation efforts—of data breaches
- Averting reputational damage to the organization, especially with regards to lost customer data
- Preventing loss of capital, intellectual property and other privileged company information

In today's world of constant connectivity and potential for headline risk and direct impact to the bottom line, cybersecurity is a key focal point for many organizations and frequently appears on the top of many board agendas. Several factors drive the increased attention paid to cybersecurity issues, including changes in the following: the overall threat landscape, technology, regulatory environments, both social and corporate.

Banks and capital markets firms are at particular risk as a result of the types of information they are entrusted with and the integral function they serve within the global economy. Additionally, regulatory agencies including the SEC, OCC, FINRA, etc., have provided organizations with requirements and guidance on expectations they are held accountable for in relation to the privacy and security of customer information.

The capabilities and techniques utilized by hackers are continuously improving and evolving, especially concerning targeting specific information, individuals, or nations. New methods are constantly developed by increasingly sophisticated and well-funded hackers who target companies not only through networks directly, but also through connections with key suppliers and technology partners. The consequences of lapse in security may be disastrous to an organization, and its overall reputation may be materially impacted. It is critical for all organizations to remain vigilant and up to date regarding recent protection criteria.

How Internal Audit can help:

- Perform a top-down risk assessment around the organization's cybersecurity process using industry standards as a guide and provide recommendations for process improvements
- Review existing processes to assess whether management considers the threats posed in the constantly evolving environment
- Assess implementation of revised technology security models, such as multilayered defenses, enhanced detection methods, and encryption of data leaving the network
- Assess third-party security providers to evaluate the extent to which they are addressing the most current risks completely and sufficiently
- Assist various divisions of the organization in understanding the level of internal control the firm has over its data

7 Third-party relationships/ vendor management

Drivers:

- Increasing oversight of third-party relationships and vendors
- Improving contract governance and creating more effective contractual self-reporting processes
- Preventing or detecting risk management failures at third-parties in a timely fashion

In order to boost productivity and efficiency, banks and capital markets firms have increasingly become reliant on third-parties to carry out critical business functions. Utilizing third-parties exposes an organization to numerous risks and potential failures that may lead to the following: fines, regulatory sanctions, lawsuits, operational bans, reputational damage, etc.

The OCC expects banks to practice effective risk management regardless of whether the bank performs the activity internally or through a third-party. An effective risk management process includes (1) performing adequate due diligence; (2) developing and implementing controls and processes to ensure risks are properly measured, monitored, and controlled; and (3) developing and implementing appropriate performance monitoring and review systems.

A bank's use of third-parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and complies with applicable laws. In addition, the updated controls framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO 2013) that took effect in December 2014 includes extensive guidance and points of focus relative to third-party service providers' significant impact on an organization's system of internal controls.

A third-party often has access to an organization's networks, which increases the possibility of data breaches. In addition, organizations may be unaware that a third-party is employing subcontractors who may be lax in their business and compliance efforts. Finally, a third-party may operate in an environment of regulatory uncertainty, thus exposing the contracting organization to further risks. Given all these factors, banks and capital markets firms must ensure that they adequately assess the cost-benefit of contracting with third-parties to ensure they are receiving the greatest benefit from these external relationships.

How Internal Audit can help:

- Review third-party identification, due diligence, selection, onboarding, and monitoring processes and controls
- Evaluate contract management processes used by management to track third-party relationships
- Consider whether it is necessary to exercise right-to-audit clauses
- Assess and recommend enforcement of third-party compliance with the organization's information security standards
- Assist with the development, implementation, and calibration of a continuous monitoring system for self-reporting of incidents from third-party business partners

8 Continuous risk assessment

Drivers:

- Developing processes to assess and address changing and emerging risks
- Increasing the frequency of risk refresh practices to ensure that resources are allocated appropriately to focus on areas of higher risk to the organization

Typically, an annual risk assessment sets an internal audit function's agenda for the upcoming year. However, banks and capital markets firms face an increasing number of unique risks that may change on a real-time basis throughout the year, thus leading this annual risk assessment process to become obsolete.

One effective approach to meet these challenges is to perform or update the internal audit risk assessment on a regular basis. Internal audit may establish mechanisms to periodically refresh its understanding of risk through the implementation of quarterly updates or ongoing meetings with business unit stakeholders to identify changes in the business' operations that may create new risk. In addition, internal audit should keep abreast of new rules and regulations that may impact the organization through regular monitoring of the changing regulatory environment. The goal of this approach is to have a more real-time view of the organization's risk profile.

How Internal Audit can help:

- Pilot continuous risk assessments for a subgroup of business units and assess its applicability to the internal audit's risk assessment and resulting audit plan
- Meet with business unit stakeholders on a regularly recurring basis to identify when changes to the business's operations may create new risk

9 Use of data analytics and continuous auditing

Drivers:

- Enabling real-time, continuous risk management
- Improving overall efficiency of internal audits being performed
- Taking a deeper dive into key risk areas through analysis of data
- Reducing costs involved in auditing and monitoring
- Enabling early detection of potential fraud, errors, and abuse

In recent years, data analytics assisted in revolutionizing the way in which banks and capital markets firms assess and monitor risk, especially in terms of efficiently expanding the scope of audits and improving audit coverage. Data analytics and continuous auditing assist internal audit functions in simplifying and improving their audit processes, which results in higher-quality audits and tangible value to the business. With data analytics, organizations have the ability to review every transaction—not just samples—and conduct efficient analysis while gaining greater coverage over the activities under review.

As organizations increasingly deploy analytical tools to meet regulators' increasing demands and to identify opportunities for operational efficiency, internal auditors will need to integrate data analysis into their core audit activities. By doing so, internal auditors will be able to assess risk on a continuous basis, in real time. Such tools may be used across many internal audit focus areas including anti-money laundering/ suspicious activity reporting, identification of trading activity anomalies, and identification of missing/inconsistent data, to name just a few. Despite material investment in data analytics and risk measurement, there still remains significant potential for internal audit to assess risk related to customer acquisition and profitability, products and pricing, regulatory reporting, risk underwriting, portfolio management, and fraud detection.

How Internal Audit can help:

- Assist in creating automated extract, transform, and load (ETL) processes, along with system-generated analytics and dashboards monitored by the business against specified risk criteria
- Assess the alignment of the company's strategic goals and objectives with risk management practices and monitoring and prioritization of the strategic objectives and risks on an ongoing basis
- Promote data analytics-enabled audit programs designed to assess the underlying data analysis and reporting of risk at the business level
- Implement automated auditing focused on root-cause analysis and management's responses to risks, including business anomalies and trigger events

10 Internal Audit talent recruitment and retention

Drivers:

- Increased participation of internal audit in strategic initiatives requiring specialized knowledge
- Expanded role of internal audit, including providing opinions on the risk management and compliance functions
- Increasing complexity of business processes, practices, and governance programs requiring independent review and challenge
- Shortage of qualified personnel within the industry

Increasingly, internal auditors are called upon to expand their presence within the organization and serve as a strategic partner to the business. This trend is driven in large part by the sheer volume of new regulatory requirements stemming from the Dodd-Frank Wall Street Reform and Consumer Protection Act to various regulations issued by the CFPB. There is a growing need for individuals with quantitative and technical skill sets (including backgrounds in enterprise risk management, model validation, vendor risk management, anti-money laundering, etc.) who can understand, test, and evaluate the business's processes against these new requirements and effectively challenge the first and second lines of defense

Internal audit functions are encountering a growing skills gap and increased competition for scarce resources within the industry. If internal audit functions are to successfully execute on their growing mandate, they will need access to talented subject matter professionals with knowledge of the industry and the organization's evolving risk profile. Organizations have several options to fulfill their internal audit needs, including comprehensive training, hiring full-time resources, outsourcing, and cosourcing. Organizations also face the challenge of retaining top talent and ensuring adequate succession plans are in place for senior management within the internal audit function.

What Internal Audit may do:

- Undertake a skills assessment on a periodic basis and identify where additional training or external resources may be necessary to achieve the internal audit plan and function's objectives
- Implement a rotational program to encourage active involvement by others within the organization
- Assess resource needs as internal audit becomes further embedded within the organization and the business's strategic initiatives
- Provide relevant training and development programs aligned with regulatory developments, as well as with wider business objectives beyond compliance
- Build relationships with external service providers to leverage subject matter professionals when needed

About KPMG's Internal Audit, Risk and Compliance Services practice

KPMG's Internal Audit, Risk and Compliance Services practice can help enhance the efficiency and effectiveness of internal audit functions, enterprise risk management programs, reviews of third-party relationships, regulatory compliance, governance, and sustainability initiatives. Our experienced partners and professionals bring deep technical and industry experience, allowing you to strengthen your key governance, risk management, and compliance efforts while at the same time enhancing your business performance.

KPMG's Internal Audit, Risk and Compliance Services practice can help you navigate the complex demands of regulators, directors, audit committees, executive management, and other key stakeholders and assist you in transforming disruptive marketplace and regulatory forces into strategic advantage.

Contact us

Sudhir Arvind
Partner, IARCS
T.: +971-24014833
E: sarvind@kpmg.com

Harikrishnan Janakiraman
Director, IARCS
T: +971-44248921
E: hjanakiraman@kpmg.com

kpmg.com