KPMG
cutting through complexity

GOVERNANCE, RISK AND COMPLIANCE SERVICES

The new internal audit charter

Defining the next generation CAEs

kpmg.com/in

The Companies Act 2013, ('the Act') ushers in a new era of corporate governance and transparency in the Indian corporate sector. The Securities and Exchange Board of India (SEBI) with the objective to align its provisions to the recently notified provisions of the Companies Act, 2013 has specifically reviewed clause 49 of the Listing Agreement, to adopt leading industry practices on corporate governance and to make the corporate governance framework more effective.

With requirements of these norms warranting organisations to provide assurance to the Board of Directors and Audit Committees on adequacy of internal financial controls, effective risk management processes, Anti-fraud controls and effective legal compliance framework, the Internal Auditor would need to review and re-define its role and fulfill its role as an important vehicle and an enabler of good corporate governance.

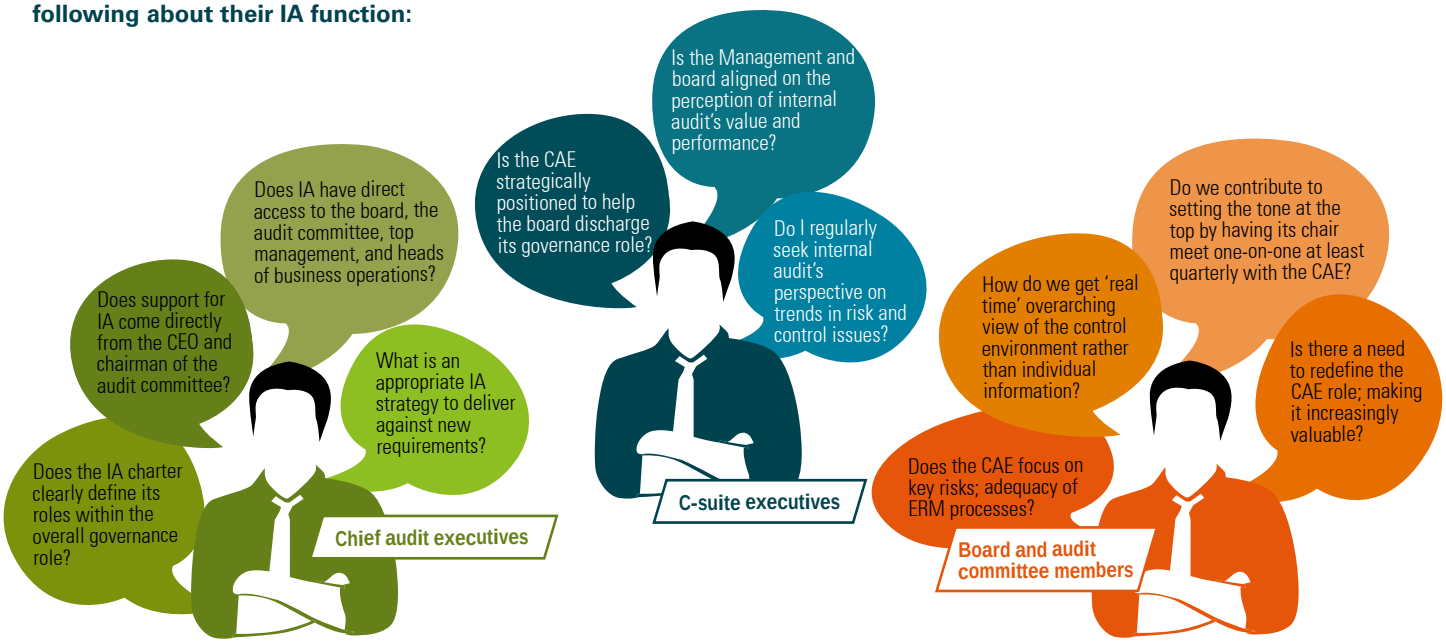
Why the Internal Audit function is suitably positioned to be an enabler of good corporate governance?

- Third line of defense: Plays an integral role in the governance structure aligned with stakeholders, clearly articulated in its mandate and widely understood throughout the organisation.
- More than a compliance function; it is recognised by business leaders as a function providing quality challenge.
- Sound understanding of business strategy and the associated risks, ability to challenge the control environment and infrastructure supporting the strategy, visibility across the various functional areas/ business units.
- Builds a strategic (two to three years) plan, developed in collaboration with the management, aligned to the organisation's risk profile.
- Structured to enable both the maintenance of independence and objectivity, as well as proximity to the business, to establish and maintain relationships with an in-depth understanding of the business.
- Dynamic processes, through integrated quality assurance and learning programs.

Going forward, the role of the Internal Audit Function is expected to become much more onerous as the board, management and independent directors seek increased comfort from an Internal Auditor on newer areas to comply with their oversight responsibility and legal duties. It is set to evolve into a more extensive, outward, forward looking and continuous activity playing an enhanced role in 'Integrated Assurance' - an activity to outline who provides assurance on what aspects of the entire assurance universe. This new purpose, authority, and responsibility of the internal audit activity must be formally defined in the new internal audit charter and presented to the senior management and the board for approval.

However, while Corporate India is looking to their internal auditors to help deliver a more sustainable, efficient and effective audit function. One that fully aligns with the new governance needs and expectations, there is ambiguity in the minds of the board, audit committee members, CXOs and Internal Auditors on what changes would be needed in their roles to fulfill these new requirements.

Chief audit executives (CAEs), executive management, the board and audit committees should be considering the following about their IA function:



As companies raise the bar on their own performance to contend with the greater regulatory and stakeholder expectations, it also raises the bar on Internal Audit Function. This whitepaper discusses **four themes** which would now form part of the new Internal Audit Charter to support the organisation and the stakeholders meet the expectations of the new Companies Act 2013 – raising the Bar on Governance. Here, we attempt to redefine the internal audit charter from the perspective of governance stakeholders and build what we call the **'New Performance Continuum'** for the Chief Audit Executive (CAE) in the wake of the changed environment. With these new expectations, it is also necessary for Internal Auditors to review their methodology and include specific procedures to address these changes. We have also discussed some of the steps and procedures which should find place in new audit plans, roles and responsibilities for the Internal Auditor.

01
Mandatory reporting on internal financial controls

The Companies Act 2013 requires the Directors report for listed companies, including public companies with paid up capital of INR25 crores or more, and auditors report for all companies to comment on whether the company has adequate internal financial controls system in place and operating effectiveness for such controls. For this purpose, the term 'internal financial controls' means the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information.

Although the ambit of internal financial control for Public companies with paid-up capital of over INR25 crores is limited to internal controls over financial reporting, given the fact that the Statutory Auditors have to comment on the operating effectiveness of internal financial controls (in its entirety, and not just internal controls over financial reporting), and the Audit Committee is entrusted with evaluating internal financial controls (both operational and financial), it appears that **all companies** will need to lay down internal financial controls covering its operations, reporting (financial and non-financial) and compliance responsibilities; and not just over financial reporting. The discussion draft issued by The Institute of Chartered Accountants (ICAI) as guidance to Statutory Auditors has indicated using the COSO framework, as the basis on which internal financial controls will be evaluated.

Therefore, the Act has significantly expanded applicability of internal financial controls to cover all aspects of operations of the company. Having evaluated their business needs and capabilities, business leaders would now need to embed internal controls monitoring their operations, reporting and compliance processes, as opposed to financial reporting only. Organisations would need to shift from point in time testing to ongoing testing embedded within the business processes.

Assess and evaluate 'Tone at the top'	• Review the management's philosophy and operating style and promote effective internal financial controls. • Check whether sound integrity and ethical values, particularly of the top management, are developed and understood. • Attempt to ensure that the Board or audit committee understands and exercises oversight responsibility over financial reporting and internal control. • Aim to ensure presence of defined policies and procedures aligned to the Company philosophy.
Develop an internal control framework	• Internal control framework based on COSO 2013 – Entity level and operations control, try to ensure holistic coverage of operational, financial and fraud risks designed in accordance with the COSO/ COBIT Frameworks. • Mapping of various operating processes/sub-process and activities at an organisation level; clearly defined workflows in line with current operating practices. • Conduct a qualitative assessment of existing documents to meet current business operations. • Identify gaps in availability/adequacy of existing documentation compared to requirements of the COSO framework. • Updated Process documents covering various components of the COSO framework. • Defined roles and responsibilities to consistently meet compliance to monitoring and reporting requirements of COSO framework.
Develop a combined assurance plan	• Develop a combined Assurance Plan for risk management and continuous monitoring through self-assessment. • Create a repository of risk and controls to help ensure identification and coverage across all financial and operating risks. (Strategic, Operational, Reputational, Financial and Fraud Risks). • Evaluate, document and prioritise risks across the organisation / business segments. • Create a reporting, monitoring and escalation framework to provide the desired level of assurance to the senior management. • Holistic risk assessment across various assertions defined under the COSO Framework.
Test the operating effectiveness of internal financial controls	• Assessment of the operating efficiencies of the process design and operating controls. • Assess the effectiveness of the Internal Control System and identification of gaps at a design and operating effectiveness level. • Implement effective management assurance through self-assessment programmes. • Continuous control monitoring and assurance through data analytics/ control dashboards. • Assist management's assessment of design of controls over business operations. • Enable evaluation of operating effectiveness and deviation identification.

The Act places a stronger emphasis than before on the role of the Audit Committee on internal financial controls and risk management. Given the importance of these areas, internal audit's assurance role is very important in helping audit committee directors fulfill their oversight responsibility and legal duties.

02
Strengthening enterprise risk assessment processes

Risk management is a central part of any organisation's strategic management. Successful organisations seek to integrate risk management and internal control into all activities, through a framework of risk identification, risk assessment and risk response.

As per the Companies Act 2013, there are specific requirements that a company needs to comply with in respect to Enterprise Risk Management. In addition, the board and audit committee have been vested with specific responsibilities in assessing the robustness of risk management policy, process and systems:

- **Section 134:** The Board of Director's report must include a statement indicating development and implementation of a risk management policy for the company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the company.
- **Section 177:** The audit committee shall act in accordance with the terms of reference specified in writing by the board, which shall, inter alia, include evaluation of risk management systems.
- **Schedule IV:** Independent directors should satisfy themselves that systems of risk management are robust and defensible.
- Also, the revised **Clause 49** of the Listing Agreement from SEBI widens the requirements for risk management. It requires the board to be responsible for framing, implementing and monitoring the risk management plan for the company.

Internal audit is third line of defense, which through its risk based approach provides reasonable independent assurance to the organisation's board of directors and senior management on the effectiveness of risk management processes. In organisations where risk management implementation is in its initial stages, the role of internal audit is often that of a catalyst or facilitator to help foster development of the organisation's risk management process. Further, the more risk mature the organization is, it is better for the internal audit function to provide a realistic picture to the board on risk management against its strategic objectives.

Key Considerations for the Chief Risk Officer (CRO)

Provide credible risk governance.

Inputs to strategy formulation; integrate risk management and strategy execution.

Aggregate information to identify operational control weaknesses .

Identify risks presenting the most significant risks to shareholder value.

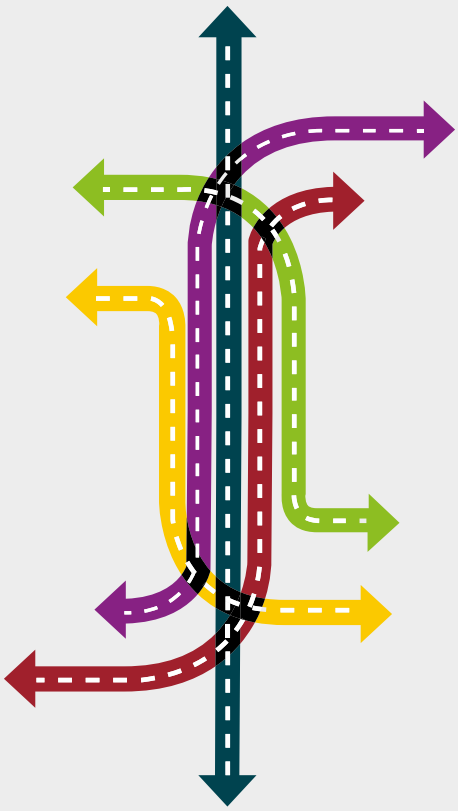
Build a risk management dashboard .

Use behavioural change management techniques to maintain risk awareness capabilities.

Coordinate with assurance providers to provide an opinion on the control environment.

Develop prudent risk management techniques to address key risks, and establish sufficient monitoring of strategic risk 'signposts' to identify risk occurrences in time.

View risk management as a core competency and try to ensure that auditors receive appropriate training on risk and risk manage-ment practices.



CAE response

Linking risk appetite to the IA's planning and reporting: adopt a risk-based audit plan.

Dynamic audit planning that factors in rapid response to emerging risks while helping ensure coverage of core processes and key controls.

Build consensus: assess risks to future growth (value creation) instead of solely focussing on the protection of existing assets.

Facilitate taking a 'portfolio' view of risk: enterprise wide response emphasising on cross-departmental, cross functional perspectives and sharing of lessons.

Educating audit committees and management on the value of effective risk management and the role internal auditors can play to help enhance that value.

Build robust risk mitigation process; different scenarios need to be assessed and stress-tested.

Expand the internal audit risk assessment process: include an evaluation of the risks embedded in the organisation's core business strategies.

Leverage continuous and anticipatory auditing processes, with strong awareness of the external environment.

CAE's Evolving Role: Business Case for 'Integrated Assurance'

Current challenge for the CAE is identifying and understanding the assurance universe across internal audit, the extent of consideration of other assurance providers in internal audit planning and execution, duplication of work by different assurance functions creating a 'nuisance factor' within the business and contradictory views given to executive management.

Internal Audit will be expected to 'connect the dots' in order to facilitate the development of an integrated assurance framework. Going forward, executive management will task the CAE with leading the risk convergence initiative at the organisation level.

Benefits will include a common risk vocabulary and consistent reporting from each of the key oversight functions (risk management, compliance, internal audit, SOX, EH&S, etc) to executive management and the Board. It would also result in cost savings as redundant activities are eliminated and common information is shared across the various oversight groups.

Internal Audit function must align its activities with the organisation's key strategies and critical risks – must be driven from the top with input from the executive management and the Board. It should be coordinated with other key oversight functions. Regardless of whether risk management and internal audit operate as distinct and separate units, or are closely aligned, it is imperative that they leverage off each other, continually developing knowledge and awareness of the environments in which they operate. They must work within the same risk management framework and conduct dialogue to continually question each other's perspective of the nature and severity of the risk profile.

03
Assessing fraud risk vulnerabilities

Globalisation has not only led to obsolete geographical boundaries, but has also increased the scale and complexity of today's business environment. It has further been complicated by continual changes in the business environment, mounting competition and multitude of regulations creating significant pressures on management to effectively maintain oversight of all operations. These challenging scenarios create various vulnerabilities in systems, procedures and frameworks for manipulation and frauds.

Fraud negatively impacts the organisation in many ways including financial, reputational, psychological and social implications. Depending on the severity of loss, organisations can be irreparably harmed due to the financial impact of the fraudulent activity. The incentives and pressures to commit frauds have always existed both within and outside the organisation. The opportunity to commit fraud arises when the fraudsters spot a weak link in the oversight process, inadequate controls, lack of proper accountability, unrestrained power to certain individuals, inadequate segregation and rotation of duties, excessive trust etc.

Organisations can most influence the opportunity element by specifying internal controls and procedures that avoid putting anyone, internal or external, to commit fraud and detects fraudulent activity as and when it occurs. The new Act proposes vital changes in this context for the first time - it defines fraud, lays down severe penalties for delinquency, fixes extensive responsibility for senior management, independent Directors and auditors, introduces the establishment of vigil mechanism and accords statutory status to Serious Fraud Investigation Office (SFIO).

- Section 447 of the Act provides a specific definition of fraud and also makes extensive provisions for penalising fraudulent activities. **Fraud includes any act, omission, concealment of any fact or abuse of the position committed by any person, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss**.
- Under the new act, liability and punishment for fraud is extended to every individual who has been a party to it deliberately, including the auditors of the company
- Companies are also required to establish a vigil mechanism for directors and employees to report genuine concerns, even directly to the chairperson of the Audit Committee for appropriate cases.
- The mechanism should provide for adequate safeguards against victimisation of persons who use such mechanism. Importantly, the details of such mechanism are required to be disclosed by the company on its website and in the Board's report.
- The directors' responsibility statement is required to include a confirmation regarding proper and sufficient care for the maintenance of adequate accounting records for safeguarding the assets of the company and for preventing and detecting fraud and other irregularities.

In light of the above, the companies will have to make sure they have adequate processes, controls and oversight mechanisms to ensure that there are adequate fraud prevention controls. The primary responsibility for prevention and detection of fraud rests with management and those charged with governance. Establishing a fraud risk management procedures would be of importance for preventing fraudulent situations and enabling timely and due monitoring and oversight by the directors.

Internal audit is in a suitable position to identify potentially fraudulent situations during the course of the audit and thus plays a strong role in preventing fraud and other illegal acts. While external auditors focus on misstatements in the financial statements that are material, internal auditors are often in a better position to detect the symptoms that accompany fraud. Internal auditors usually have continual presence in the organisation that provides them with a better understanding of the organisation and its control systems.

Therefore, the CAE will now need to take responsibility over the adequacy of fraud prevention/ mitigation controls in business processes. He will have to consider fraud procedures as part of every audit. He can no longer take shelter that the IA function is not responsible for preventing and detecting fraud.

Creation of 'tone at the top' which communicates that fraud will not be accepted in any form.

Implement policies/code of conduct that encourage ethical behavior by employees, board members and external business partners.

Establish an independent vigil mechanism for directors and employees to report concerns, even violation of policies.

6

Actions to be taken by the Board/Audit Committee for fraud risk mitigation

Monitor the organisation's fraud risk management process that helps ensure action/ resolution on all reported fraud/ violations.

Create effective governance model for deterrence of fraud; consider all aspects of board governance including processes controlling board information, agenda, access to management etc.

Oversight of executive management's compliance with appropriate financial reporting and for preventing executive management's override of controls or other inappropriate influence over the financial reporting process.

Fraud risk and the role of a CAE

Proactive auditing to look for misappropriation and misrepresentation

- **Examining and evaluating the adequacy and effectiveness of internal controls that might address fraud risks include:**
  - Controls over significant, unusual transactions
  - Controls over adjustments in the period-end financial reporting process
  - Controls over related party transactions
  - Controls related to significant management estimates
  - Controls that mitigate incentives for, and pressures on, management to falsify or inappropriately manage financial results.
- **Fraud Detection activities include** potential fraud indicators in the Risk Control Matrix/Audit Program. Gather sufficient knowledge of fraud to identify red flags indicating fraud that may have been committed, the techniques used to commit fraud, and the various fraud schemes and scenarios associated with the activities reviewed.
  - Leverage data mining and data analytics to find unusual items and perform detailed analyses of high risk accounts and transactions.
- **Establish effective fraud prevention measures based on a company's SWOT analysis.**
  - Define robust control activities i.e., policies and procedures for business processes, including appropriate authority limits and segregation of incompatible duties, employee training etc.
- **Test operating effectiveness of fraud prevention and detection controls.**
- **Identify relevant fraud risk factors:** understand organisations external and internal business environment. Review the documentation of previous and suspected frauds, frauds at similar organisations, root cause analysis and control improvement recommendations, monitoring the reporting/whistleblower hotline, and providing ethics training sessions.
- **Map existing controls to potential fraud schemes and carry out a gap assessment:** identify preventive and detective controls in place to address fraud risks and likelihood and significance of each potential fraud.
  - Entity level anti-fraud controls such as whistleblower hotline, whistleblower protection policy, board oversight, results of continuous monitoring, code of conduct are important elements in the exercise.
- **Discuss management concerns and communication protocol in case of a fraud.**

04
Comprehensive legal compliance framework

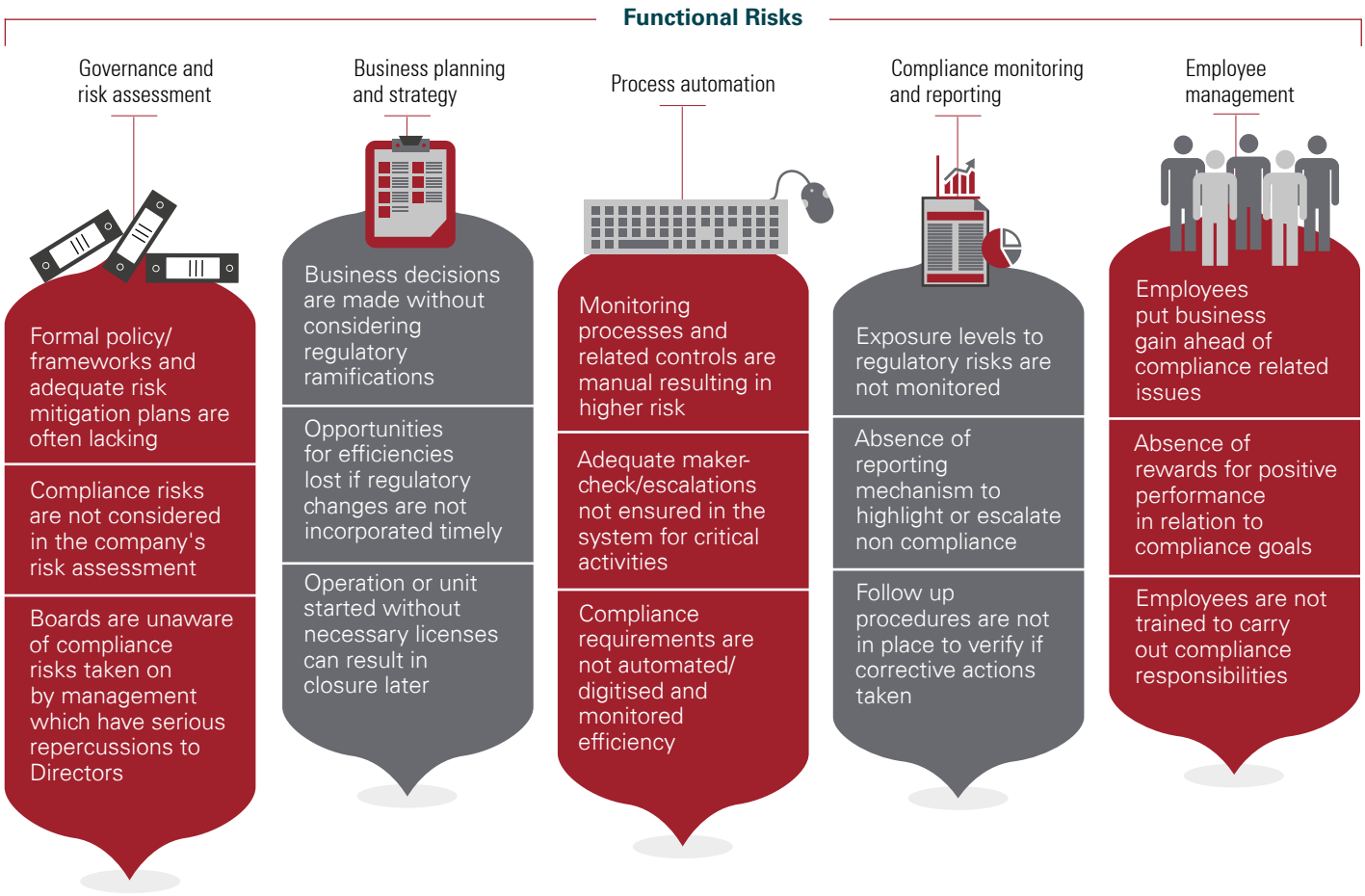
India as a country is neither short of laws nor legislatures. What is lacking is the enforcement of and compliance with these laws. The Companies Act 2013 is a step in this direction for making corporate India more accountable. Together with Clause 49 of the listing agreement, the government is seeking to make Directors of companies responsible for devising proper system to help ensure compliance with 'Provisions of All Applicable Laws' and that such systems are adequate and operating effectively. The Boards now need to periodically review compliance reports of all laws applicable to the company, prepared by the company, as well as steps taken by the company to rectify instances of non-compliance.

Key considerations for the Board/Audit Committee

- Whether the organisation has developed an awareness of the various compliance programs to which it is subject, and does it get an integrated view so as to report violations, if any.
- How are we identifying, monitoring, and adjusting for emerging compliance risks and requirements?
- How can the board determine whether resources devoted to compliance programs are adequate and aligned with the organisation's risk appetite?
- What knowledge and experience does the board currently lack in order to understand and effectively oversee our compliance programs?
- How are senior leaders accountable for fostering a culture of compliance in their performance goals? How are they performing?
- How are we monitoring legislative changes at the global and national level? How is compliance integrated into geographical growth strategies.
- Where have we fallen short in compliance reporting, and how are we addressing the problem?

An all-encompassing framework is now mandatory to ensure that applicable laws are identified, mapped to the respective process owners across functions and locations and that the company can demonstrate that not only are all applicable laws being complied with, any non-compliances which can and will occur have been properly dealt with.

Multiple risks exist in monitoring the Legal and Regulatory Compliance function



In order to implement a robust legal compliance framework, companies need to consider the following elements:

- Comprehensive Legal Compliance Framework for all applicable laws
- Well defined roles and responsibilities for compliances across locations & functions
- Technology enabled tools & databases to ensure compliance
- Trainings to be rolled out to employees on the compliance framework requirements
- A robust review & reporting mechanism over compliance status

The Legal compliance framework needs to cover three key elements:

1. **Governance level:** This includes the compliance around organisation structure, policies and procedures documents, well defined roles and responsibilities a risk assessment of regulatory risks and a well-defined reporting structure.
2. **Operating level:** The company needs to relook at its business practices to ensure they are aligned with all applicable laws as not everything can be covered by a simple check list. Given the size and scale of companies an automated tool will also be required to ensure compliance monitoring is effective. Document retention and training will also be key to ensuring proper compliance.
3. **Monitoring level:** Finally, companies need to ensure proper monitoring systems are in place which would include MIS and reporting, audits, inspections and site visits if required, self-certification, third party compliance programs and remediation plans and processes for non-compliances.

With the enactment of the New companies Act, 2013, the Board of Directors, and in particular, the independent directors will increasingly look upon to the Internal auditors to give reasonable assurance that the Legal Compliance process is adequate and operating effectively and is suitably evidenced. With these new expectations, it will be necessary for Internal Auditors to review their methodology to ensure robust processes for ensuring comprehensive compliance with applicable laws and regulations.

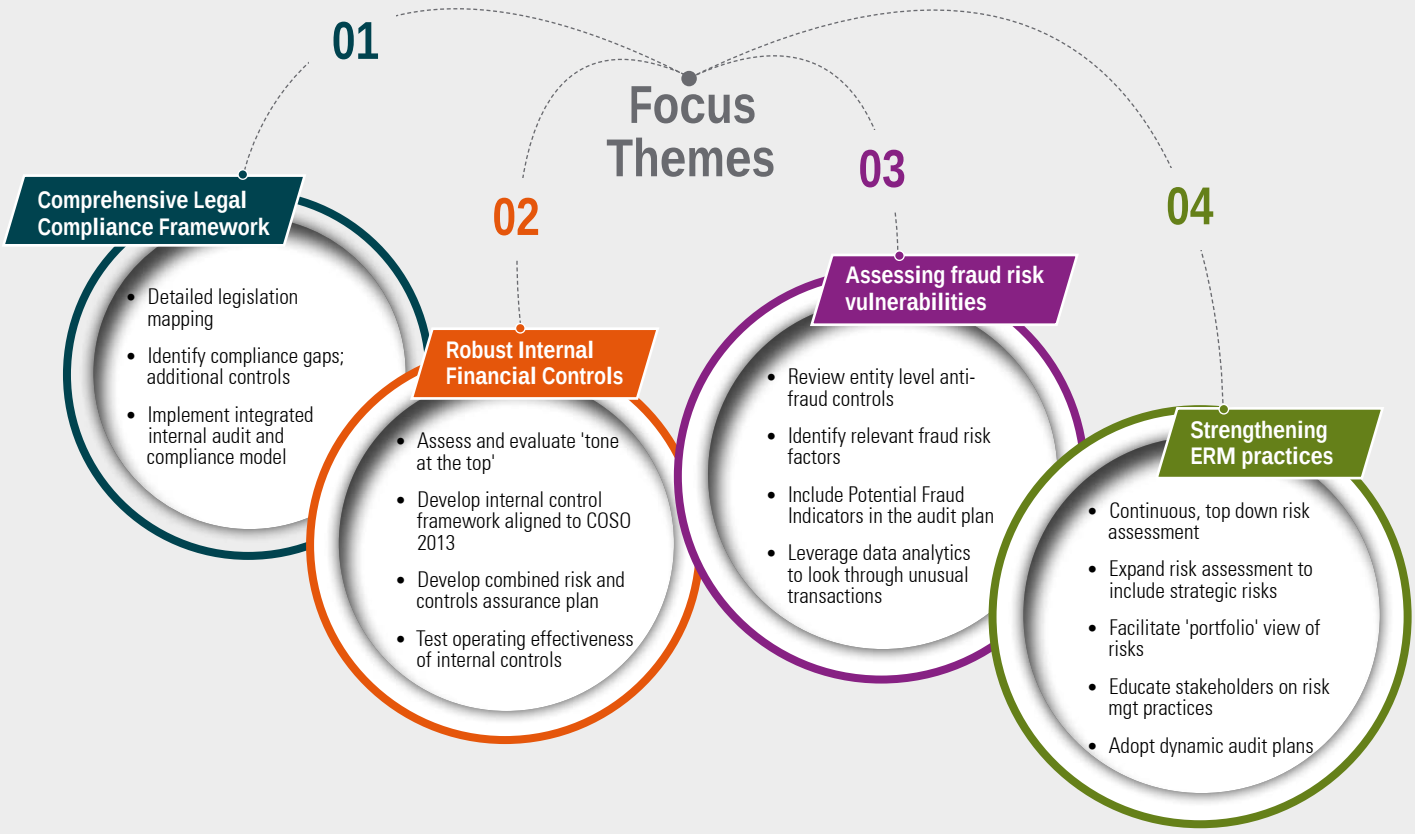
Rolling Out an Effective Compliance Framework

Role of the CAE

Map the legislations to the existence of a policy and develop a risk map. Also, provide inputs on additional controls required which are arising from amendments to, or new legislation. The three major keys in such an approach are:

- Evaluate current business operations and the compliance implications. This step identifies compliance resources, internal audit resources, technologies and actively develops an initial baseline cost of compliance and internal audit.
- Analyse the effectiveness of the existing compliance and internal audit programs against existing risks and identify any compliance gaps and potential needs for additional controls and elimination of duplicative services.
- Implement 'an integrated operating model' for compliance and internal audit:
  - An integrated compliance and internal audit function which facilitates a more consistent approach across the organisation ensuring standards are consistently being met and any duplication and unnecessary activities are reduced, if not eliminated and therefore, costs are reduced.
  - Compliance management controls can now be assessed against a common enterprise-wide standard that replaced the individual standards in the old model.
  - An integrated structure creates open dialogues and increases awareness of operational risk and compliance issues which fosters a stronger risk and compliance management culture.

Therefore, the internal audit's new charter needs to be launched, anchored on four key themes



The new performance continnum: changed environment is expected to drive the CAE to become distinctive on key dimensions

It is a fact that the Internal Audit function has evolved and today's Internal Audit function is expected to assist the organisation by highlighting leading industry practices, acting as independent advisors to management and the board, actively participating in enterprise risk management activities, including sustainability, and by promoting good governance. Looking to the future, Internal Audit departments that maintain alignment with the changing risk profile of their organisations and the evolving needs and expectations of their key stakeholders will be more successful. Internal Audit needs to staff individuals who are senior and experienced enough, with sufficient business understanding, to apply opinions, judgment and challenge to the business on a broad array of topics. Internal Audit needs to have an effective means of identifying skills and competencies required to deliver its annual plan, identifying and filling gaps and being responsive to the rapidly changing risk profile of the organisation.

Under-performing		Excelling/Among the best
Costly silos	Integrated assurance	Single view
Information-heavy reports	Internal audit's impact	The timely 'so what'
Accounting and audit skills	The right people	Multiple, specialised tracks
Bottom-up	Risk-based approach	Top down
Sporadic use	Continuous auditing and technology	Analyse for early warnings
Compliance function	Seat at the table	Audit committee/BOD support
Controls overview	Expanded services portfolio	Risk mitigation, data analytics, supply chain, fraud investigation

Source: KPMG International analysis

The internal audit function will have to transform through four key actions

Make strategic investments

- **Subject matter experts** used for specific technical reviews and provide objective views on special cases
- Strengthen internal capabilities by selectively **upgrading talent and making knowledge investments**
- Invest in **developing innovative solutions** for end clients
- Invest in **technology**; consider **strategic alliances.**

01

Expand/rebalance services portfolio

- **Deepen end-to-end capabilities** in core areas
- Transition from **value preservation to value creation**
- Internal audit plan guided and defined by **multiple stakeholders and real time inputs**
- Transition from **'assurance provider' to 'trusted advisor'**
- Deliver a **strategic vision** that aligns to stakeholder expecta¬tions.

02

Improve contribution

- **Invest** in understanding client's business, industry, operations
- Supplement core selling approaches with **end-to-end transformative big bets** and create portfolio of 'compliance' services
- Strengthen capabilities such as **end-to-end optimisation** in response to ERM, fraud risk mitigation, compliance
- **Greater alignment** with the Audit committee/Board.

03

Strengthen operations/delivery

- Provide both **positive assurance as well as exception reporting**
- Cover and report on **self-assessments process** of business and review of various **oversight functions and practices**
- Shift toward cross-functional **integrated assurance**
- **Proactively respond; force conversations.**

04