

Tailored expertise to
maximise returns
and minimise risk.



INTERNAL AUDIT – THE CHANGING LANDSCAPE



RSM IN INDIA

- RSM India (comprising of RSM Astute Consulting Group and affiliates) is consistently ranked amongst India's top 6 tax, accounting and consulting groups [International Accounting Bulletin, July 2018]
- Nationwide presence through offices in 11 key cities across India
- Multi-disciplinary personnel strength of 1,475
- International delivery capabilities

rsmindia.in

RSM AROUND THE GLOBE

- Sixth largest audit, tax and consulting network across the globe
- Annual combined fee income of US\$ 5.1 billion
- Combined staff of over 43,000 in over 800 offices across 120 countries
- RSM is the fifth largest audit, tax and consulting group in the USA

rsm.global





Internal Audit

- The Changing Landscape

PREFACE

“Business will be better or worse. We cannot do today's job with yesterday's methods and be in business tomorrow.”

– Nelson Jackson

Internal Audit function plays a very crucial role in an organisation's corporate governance framework, internal processes and controls, risk management, regulatory compliance, financial reporting and overall assisting the Board of Directors and senior management help fulfil their responsibilities towards the organisation and its stakeholders.

This role is ever expanding and in many matured organisations, it is expected that the role of Internal Audit function must spread into newer and broader areas such as sharing insights in management's strategic and transformative initiatives, facilitating 100% compliance to regulatory requirements, proactively participating in management decision making, identifying disruptive means to achieve the internal audit objectives, helping organisations reduce the overall cost of compliances, etc.

Internal audit function acts as an intelligent and agile tool available with the Audit Committee of the Board of Directors and the overall Board to discharge the duties bestowed to them by the various stakeholders. Given its onerous duties, the Board/Audit Committee heavily rely on internal audit function to provide assurance to stakeholders.

The Chief Audit Executive is expected to venture into newer areas and keep innovating and improvising its Audit Charter so that the value and benefits to the organisation are maximised. Thus, there is a definitive shift in perception of Internal Audit function from being a 'Cost Centre' to being a 'Profit Centre'.

In this booklet, we have endeavoured to touch upon the key aspects of internal audit function keeping in mind the traditional success factors, the present trends and an eye on the Future of Internal Audit in the ever-changing business environment and digital arena.

We set the tone by capturing the key expectations from relevant stakeholders, followed by understanding the evolution of internal audit over years and glancing through the current regulatory framework around internal audit and corporate governance. This

follows by some insights on how internal audit function has joined the transformation bandwagon coupled with the impact of technology on the internal audit function including a topic on the relevance and operationalisation of Data Analytics as part of Internal Audit. Lastly, we touch upon one of the core objectives of internal audits, i.e. 'Value Addition' in detail.

We hope you find this publication relevant and useful.

Happy Reading!

Table of Contents

| Sr. No. | Chapter | Pg. No. |
|---------|---|---------|
| 1 | Expectations of the Board of Directors, Audit Committee and Senior Management from Internal Audit | 1 |
| 2 | Internal Audit Evolution | 6 |
| 3 | Current Regulatory Framework Pertaining to Corporate Governance | 14 |
| 4 | Transformation of the Internal Audit Function | 22 |
| 5 | Technology Impact and Changing Dynamics of Internal Audit | 33 |
| 6 | Data Analytics – Effective Tool for Internal Auditors | 47 |
| 7 | Internal Audit Value Proposition and Value Delivery | 60 |

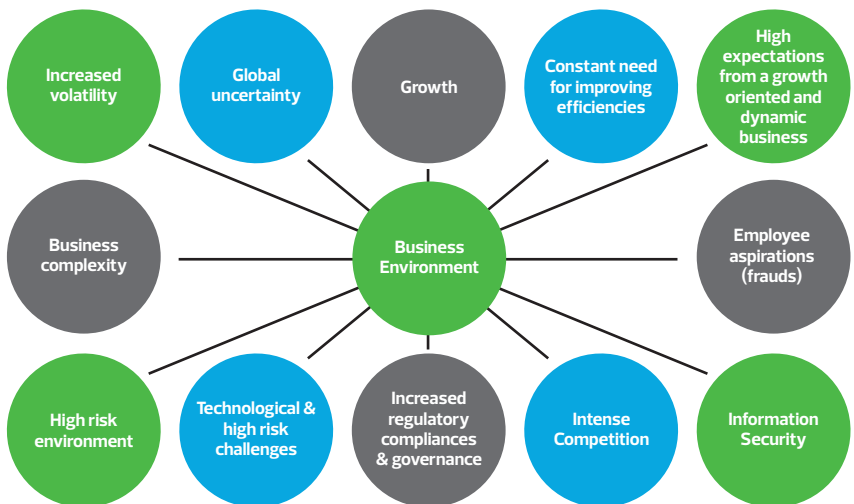
EXPECTATIONS OF THE BOARD OF DIRECTORS, AUDIT COMMITTEE AND SENIOR MANAGEMENT FROM INTERNAL AUDIT



1.1 Introduction

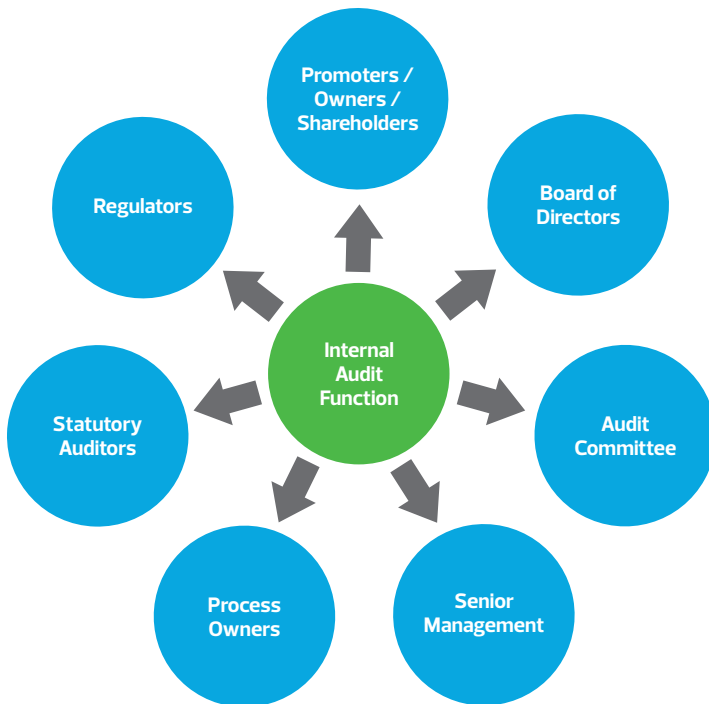
- The role of contemporary internal audit function has expanded manifolds in the recent years. This has resulted in heightened expectations of the stakeholders at different levels within an organisation.
- In a fast changing and dynamic business environment, the roles and responsibilities of the Board of Directors (BOD) and senior management of the organisations are becoming increasingly significant. Political and economic uncertainties, market volatility, dynamic business environment, technological and digital disruptions, frauds, cyber threats, increased regulatory compliances and investor demands for greater transparency have all significantly heightened and expanded the BOD's oversight responsibility.

Figure 1.1: Factors affecting business environment



- In order to meet its governance, control and risk management responsibilities and improving operational efficiencies, the internal audit function plays a pivotal role by providing continual review of business processes and risks, their operating effectiveness and valuable insights that would help the BOD and senior management to discharge their oversight duties more effectively, efficiently and in a timely manner.
- There are multiple stakeholders who heavily rely on the work of internal audit function to discharge their own obligations and therefore have diverse expectations.

Figure 1.2: Internal Audit and its key stakeholders



- 'Is internal audit function meeting the stakeholders' expectations?' This is an important question that is being discussed and deliberated across industry spectrum as we look into the future of internal audit.

1.2 Key Expectations from Internal Audit Function

- Exhibit deep understanding of the organisation's industry and business environment, its processes, functions and operations and changes therein.
- Develop robust internal audit plans that effectively evaluate the organisation's strategic, operational, financial and compliance risks.
- Ensure internal audit plan is aligned to the organisation's risk assessment and addresses not only existing risks but even emerging risks due to new markets/new products, Mergers & Acquisitions, Cloud Computing, Social Media, Robotic Process Automations, Cyber Security, etc.
- Conduct independent and objective assessment of risks and controls to provide overall comfort on the state of internal financial controls, its design and operating effectiveness.
- Ensure value addition through consulting by identifying and recommending areas for cost reduction, revenue optimization and improvement in operational efficiency.
- Employ technology, tools and data analytics throughout the audit cycle to sharpen audit effectiveness and efficiency and elevate audit execution and reporting to the next level.
- Use multi-disciplinary team of professionals equipped with requisite skills, industry acumen and experience to deliver customised solutions to maximise returns and minimise risks.

- Benchmark organisation's current processes with industry best practices and suggest potential improvements.
- Provide specific, measurable, achievable, realistic and time bound (SMART) recommendations that address the root cause accurately and in a more meaningful manner.
- Focus on delivering results and implementing preventive actions, than simply uncovering problems after they occur.
- Ensure audit reports and presentations are clear, succinct, impactful and delivered on timely basis.

1.3 Conclusion

The Chief Audit Executive has to continuously assess the effectiveness of the Internal Audit function and ensure that the collective expectations of all relevant stakeholders are balanced and met with, if not exceeded.



2.1 History of Internal Audit

Internal audit demand traditionally emerged as a means of independent verification to reduce accounting errors and asset misappropriation within business organisations. It developed as an extension of the external audit role in testing the reliability of accounting records that contribute to the published financial statements. Internal auditors were seen to be playing a fairly modest role within organisations and had only a limited responsibility in the total managerial spectrum.

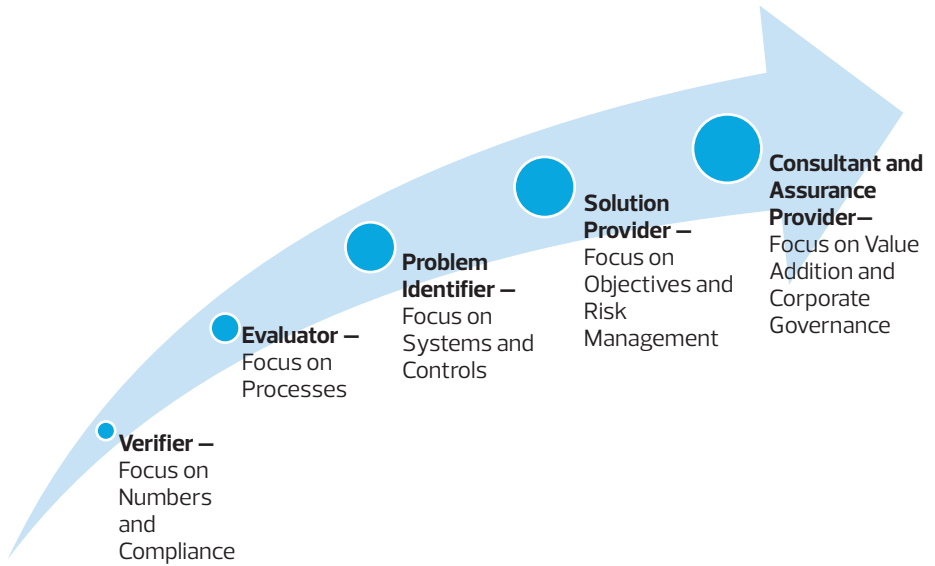
The testing role progressed to cover non-financial areas, and this equated the internal audit function to a form of internal check. Many transactions were double-checked to provide assurances that they were correct and properly authorised by laid-down procedures.

Internal audit further evolved as a probity function where it came to be more concerned about the probity aspects of the transactions, especially those involving liquid and highly movable assets such as cash, stocks, etc.

As business activities grew in size, scope and complexity, a critical need for a separate internal audit function that would verify the accounting information used for decision-making by management emerged. The widening gap between management and action made it necessary to develop a series of controls by means of which the business may be administered efficiently. Accordingly, the next stage in evolution was the segregation of audit from the finance function. The function gained organisational and professional status by employing Chief Audit Executives to lead the Internal Audit function and carry out risk based internal audits, working independently and reporting to the Audit Committee of the Board.

Currently, internal auditors are looked upon by various stakeholders as advisors and consultants to management with the objective of adding value to the organisation, including providing assurance over corporate governance and financial reporting.

Figure 2.1 Evolving Expectations from Internal Audit Function over years



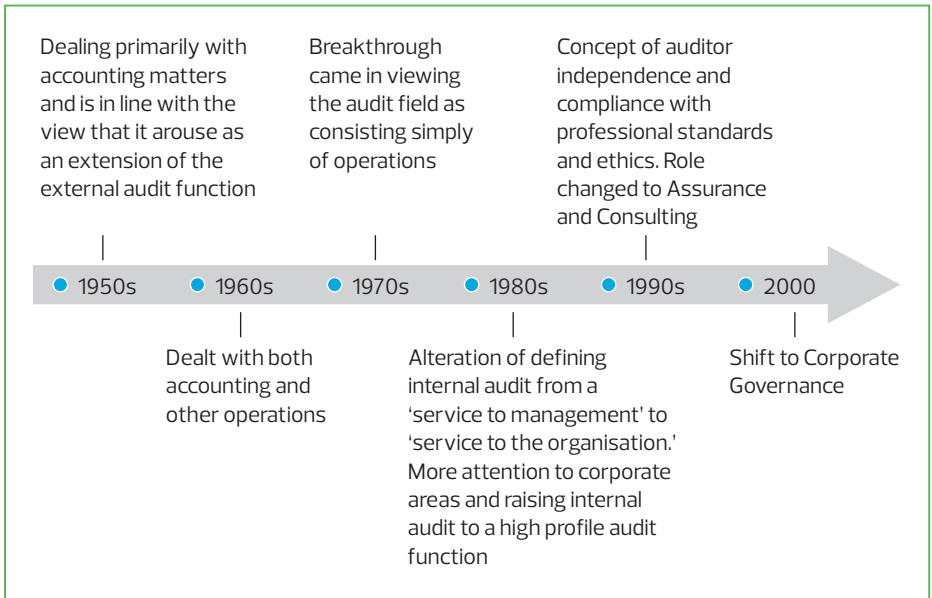
2.2 Global History

Internal Audit as defined by Institute of Internal Auditors (USA):

"Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance process."

This definition has been adopted by the Institute of Internal Auditors (India) which is affiliated to the USA Institute. The Institute of Internal Auditors (IIA) has issued various statements of responsibilities (SOR) since its inception which depicts the changing role of internal audit over last six decades as depicted in the following diagram.

Figure 2.2 Changing role of internal audit over last six decades



The IIA endorses the 'Three Lines of Defence' model as a way of explaining the relationship between these functions and as a guide to how responsibilities should be divided:

1. First line of defence – functions that own and manage risk.
2. Second line of defence – functions that oversee or specialise in risk management, compliance.
3. Third line of defence – functions that provide independent assurance, above all, i.e. internal audit.

2.3 Indian History

2.3.1 Companies Act

The legal recognition of internal audit in regulatory landscape can be traced back to

Manufacturing and Other Companies (Auditors Report) Order, 1988 (MAOCARO) notified by the Central Government under Companies Act, 1956 and subsequently under the Companies (Auditor’s Report) Order (CARO), 2003 and now under the Companies Act, 2013 .

The below table summarises the mandatory requirements around Internal Audit over years:

| MAOCARO (1988) | CARO (2003) | Companies Act, 2013 |
|--|---|---|
| <p>MAOCARO required external auditors to report about the internal control procedures and internal audit systems for the company:</p> <ul style="list-style-type: none"> ■ Whether they are adequate internal control procedures commensurate with the size of the company and the nature of its business are in place for purchase of stores, raw materials including components, plant and machinery, equipment and other assets and for sale of goods exists:? ■ Whether the company has an internal audit system commensurate with its size and nature of business in case of companies having paid up capital exceeding | <p>The amended CARO, 2003 retained the same reporting requirements as in MAOCARO with certain changes as below:</p> <ul style="list-style-type: none"> ■ Whether they are adequate internal control procedures commensurate with the size of the company and the nature of its business for purchase of inventory and fixed assets and for sale of goods exists. Whether there is a continuing failure to correct major weakness in internal control. ■ Whether the company has an internal audit system commensurate with its size and nature of business in case of companies having paid | <p>The Companies Act, 2013 has given statutory recognition to the function of Internal Audit by making it mandatory for certain class of companies. As per the Rule 13 of Companies (Accounts) Rules, 2014, certain classes of companies are required to appoint internal auditors. (Refer Chapter 3 for details.)</p> |

| MAOCARO (1988) | CARO (2003) | Companies Act, 2013 |
|--|--|---------------------|
| Rs 25 lakhs at the commencement of the financial year or having average annual turnover exceeding Rs. 2 crores for a period of three consecutive financial years preceding the concerned reporting financial year? | up capital exceeding Rs. 50 lakhs at the commencement of the financial year or having average annual turnover exceeding Rs. 5 crores for a period of three consecutive financial years preceding the concerned reporting financial year? | |

The Companies Act, 2013 (which has replaced the old Companies Act of 1956) has introduced provisions to enhance the transparency in financial reporting which have resulted in greater and unprecedented accountability on the part of Board of Directors, Audit Committee, Independent Auditors and Management (including CEOs/CFOs).

2.3.2 Institute of Chartered Accountants of India

Internal Audit is not defined in the Companies Act, 2013; however it is defined in the Preface to the Standards on Internal Audit issued by The Institute of Chartered Accountants of India (ICAI) as under:

“Internal Audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity’s strategic risk management and internal control systems.”

Apart from the Preface to the Framework and Standards on Internal Audit, the Framework Governing Internal Audits and the Basic Principles of Internal Audit, the Internal Audit Standards Board of ICAI has, till date, issued 18 Standards on Internal Audit (SIAs). The SIAs aim to codify the best practices in the area of internal audit

and also serve to provide a benchmark on the performance of the internal audit services. The SIAs are currently recommendatory in nature and will become mandatory from the date yet to be notified.

The SIAs are principle based and outlines the objective of issuing the particular Standard along with the essential requirements for its compliance. Internal Auditors are expected to apply their best professional judgement in the implementation of SIAs on a "substance over form" basis. In addition to the SIAs, for the benefit of its members and internal auditors, the Internal Audit Standards Board of ICAI has issued several industry specific internal audit guides highlighting the peculiar aspects of those industries. All these guides have been consolidated in the "Compendium of Industry Specific Internal Audit Guides".

The list of existing SIAs is given below.

Standards on Internal Audit

| | |
|---|--|
| SIA 210 – Managing the Internal Audit Function | SIA 220 – Conducting Overall Internal Audit Planning |
| SIA 310 – Planning the Internal Audit Assignment | SIA 320 – Internal Audit Evidence |
| SIA 330 – Internal Audit Documentation | SIA 4 – Reporting |
| SIA 5 – Sampling | SIA 6 – Analytical Procedures |
| SIA 7 – Quality Assurance in Internal Audit | SIA 8 – Terms of Internal Audit Engagement |
| SIA 9 – Communication with Management | SIA 10 – Internal Audit Evidence |
| SIA 11 – Consideration of Fraud in an Internal Audit | SIA 12 – Internal Control Evaluation |
| SIA 13 – Enterprise Risk Management | SIA 14 – Internal Audit in an Information Technology Environment |
| SIA 15 – Knowledge of the Entity and its Environment | SIA 16 – Using the Work of an Expert |
| SIA 17 – Consideration of Laws and Regulations in an Internal Audit | SIA 18 – Related Parties |

The roles and responsibilities of internal auditor as it pertains to the given topics are explained in the respective SIAs as stated above.

2.4 Conclusion

Increasing number of Chief Audit Executives are moving towards more effective and efficient ways to meet the overall internal audit objectives. These trends include formalisation of internal audit function in terms of objectives, role, responsibilities, team, scope, approach, reporting, follow up and escalation mechanism. The effectiveness of the function is enhanced by use of Digital tools, Data Analytics, Continuous Monitoring Tools, Reporting and Audit Management, Dashboards, Hybrid delivery models (combination of on-site and offshore delivery models) and leveraging work done by the first and second lines of defence, without compromising on their independence. This shift and adaptation by management and internal auditors is leading to external auditors and regulators placing higher level of reliance on management testing and assurance activities, which in turn is helping in reducing the overall cost of compliance.

CURRENT REGULATORY
FRAMEWORK PERTAINING TO
CORPORATE GOVERNANCE



3.1 The Business Imperative and Focus on Corporate Governance

We are living in a highly complex and uncertain business world. There is a growing inter-dependence among economies due to globalisation and increased cross border activities. The technological revolution and emergence of digital world has added new dimensions to this complexity with developments such as on-line sales, mobile applications, ERPs, block chain solutions, cloud computing, robotic business process automation (RPA) etc. In near future, it is expected that internet of things (IoT), machine learning (ML) and artificial intelligence (AI) will add new dimensions to businesses. The regulations and stringent attitude of the regulators has further heightened the need for compliances to the fullest extent.

The risks of fraud have increased manifold with growing aspirations, cyber-crimes and volatility of business. In the last decade, the world has witnessed high level corporate and financial frauds which shook investors' and stakeholders' confidence. The expectations of the investors, lenders and other stakeholders in terms of governance have reached unprecedented levels. This necessitated strong legislation to improve financial disclosures from corporations, prevent accounting frauds, regulate financial practices and corporate governance.

In the past few years, India too has witnessed some high profile corporate frauds which led to SEBI introducing clause 49 in the listing agreement in 2005 which required the CEO and CFO of every listed company to certify on effectiveness of the systems of internal controls. SEBI on September 2, 2015 issued the SEBI (Listing Obligations and Disclosure Requirements, LODR) Regulations, 2015 ('Listing Regulations') with an aim to consolidate and streamline the provisions of existing listing agreements for different segments of capital markets such as equity shares (including convertibles), non-convertible debt securities, etc. and disclosure norms in relation thereto, thereby ensuring better enforceability, while retaining the requirement for the CEOs/CFOs to certify on the effectiveness of the internal controls in their organisations.

The current corporate governance practices of the Indian listed corporate entities, where still a sizeable number of such entities are promoter-led, are on the verge of evolution with these corporate governance amendments.

The Companies Act, 2013 has introduced provisions to enhance the transparency in financial reporting which have resulted in greater and unprecedented accountability on the part of BOD, audit committee, independent auditors and management (including CEOs/CFOs).

The Companies Act, 2013 and the SEBI (LODR) regulations cast responsibility on BOD and audit committee for implementation and monitoring of following frameworks:

- Internal Audit
- Internal Financial controls Framework
- Enterprise Risk Management
- Fraud Risk Management
- Legal Compliance Framework

3.1.1 Mandatory Internal Audit

The Companies Act, 2013 has given statutory recognition to the function of internal audit by making it mandatory for certain class of companies. As per the Rule 13 of Companies (Accounts) Rules, 2014, certain classes of companies are required to appoint internal auditors. The table below summarises the applicability:

| Parameters of internal audit applicability | Unlisted Company (Amount in Rs. Crore) | | Listed Company |
|--|---|-----------------|---|
| | Public Company | Private Company | |
| Turnover | 200 | 200 | Always applicable irrespective of any of the parameters |
| Loans or borrowings | 100 | 100 | |
| Paid-up Share Capital | 50 | Not Applicable | |
| Deposits | 25 | Not Applicable | |

3.1.2 Implementation of Other Frameworks

The provisions of the Companies Act, 2013 have made the Board of the companies responsible for ensuring that following frameworks are put in place, monitored regularly and reported upon, as a part of overall corporate governance. The Board's responsibilities include:

| Internal Financial Controls (IFC) | Enterprise Risk Management System (ERM) | Fraud Risk Management (FRM) | Legal Compliance Framework (LCF) |
|--|---|---|---|
| <ul style="list-style-type: none"> ■ Polices and procedures to ensure efficient conduct of business <ul style="list-style-type: none"> - Safeguarding of assets - Prevention and detection of frauds and errors - Accuracy and completeness of accounting records - Timely preparation of reliable financial information | <ul style="list-style-type: none"> ■ Approving and monitoring the ERM ■ ERM includes: <ul style="list-style-type: none"> - Identification of significant risk exposures - Assessing the impact of significant risk exposures - Action plan for risk mitigation - Monitoring progress | <ul style="list-style-type: none"> ■ Preventing and detecting frauds: ■ FRM includes <ul style="list-style-type: none"> - Creating control environment - Conduct of fraud risk assessment - Establishing prevention techniques to avoid key risk - Promoting tools for reporting suspicious activities - Response to fraud allegation | <ul style="list-style-type: none"> ■ Devising proper systems to ensure compliance to applicable laws ■ LCF includes: <ul style="list-style-type: none"> - Identification of all applicable laws and their requirements - Development of system to ensure compliance - Ensuring training and awareness among employees - Monitoring compliance status |

The above requirements have also widened the roles and responsibilities of the internal audit function as to ensure that such frameworks are designed and implemented by the companies, verifying the existence and effectiveness of these frameworks, appropriate reporting, etc.

3.2 Other Important Regulatory Aspects

3.2.1 Serious Fraud Investigation Office (SFIO)

A committee on corporate governance was set-up by the Government of India under the chairmanship of Shri Naresh Chandra, former Cabinet Secretary. One of the recommendations of the Committee was setting up of Corporate Serious Fraud Office.

As per the Companies Act, 2013, SFIO is a multi-disciplinary organisation under the Ministry of Corporate Affairs, consisting of experts in the field of accountancy, forensic auditing, banking, law, information technology, investigation, company law, capital market and taxation etc. for detecting and prosecuting or recommending for prosecution white collar crimes/frauds.

Investigation into the affairs of a company is assigned to SFIO;

- a. on receipt of a report of the Registrar or inspector under section 208 of the Companies Act, 2013;
- b. on intimation of a special resolution passed by a company that its affairs are required to be investigated;
- c. in the public interest; or
- d. on request from any department of the Central Government or a State Government

3.2.2 Establishment of Vigil Mechanism

Whistle blowing means inviting the attention of the top management to

wrong doings and frauds occurring within an organisation. The term is now being heard more than ever before, as the media, corporates and the public are now becoming increasingly aware of the concept, but unfortunately until the Companies Act, 2013, there were no safeguards provided to a whistle blower.

All the listed companies or companies which accept deposits from the public or companies which have borrowed money from banks and Public Financial Institutions (PFIs) in excess of Rs.50 crores under section 177(9) read with Companies (Meetings of Board and its Powers) Rules, 2014, are required to establish a vigil mechanism for directors and employees to report genuine concerns in such manner as may be prescribed. The details of establishment of such mechanism shall be disclosed by the company on its website, if any, and in the Board's report. The vigil mechanism should also provide for adequate safeguards against victimisation of persons who use such mechanism and make provision for direct access to the chairperson of the Audit Committee in appropriate or exceptional cases.

In case of repeated frivolous complaints being filed by a director or an employee, the audit committee or the director nominated to play the role of audit committee may take suitable action against the concerned director or employee, including reprimand.

3.2.3 Introduction of provisions relating to frauds

In order to bring transparency and discipline in the corporate world to protect the interests of the shareholders and public at large, the Government has come up with more specific and clear provisions relating to fraud & fraud reporting under the Companies Act, 2013.

The Fraud provisions are in force with effect from 12 September, 2013 and the Fraud reporting provisions are brought in force with effect from 1 April, 2014 and were amended by the Companies Amendment Act, 2015. On 14 December, 2015, the Ministry of Corporate Affairs (MCA) issued a notification pertaining to reporting of frauds (Rule 13 to the Companies (Audit and Auditors) Amendment

Rules, 2015) specifying threshold value of fraud loss from a reporting standpoint. The notification states that if an auditor has "reason to believe" that fraud, which involves or could potentially involve individually an amount of rupees one crore or above, is being or has been committed against the company, the auditor needs to report the matter to the Central Government within 60 days of his or her knowledge of such a fraud. The process for doing this, includes reporting the matter to the company's Board or the Audit Committee within 2 days (of coming to know about the fraud), seeking a response from the Board or Audit Committee on the matter (within 45 days), and forwarding this response along with the auditor's own report to the Central Government (within 15 days). In case of no response from the Board or Audit Committee, the auditor's report along with the communication sent to the Board should be forwarded to the Central Government. In case of a fraud involving amounts less than Rs. one crore, the auditor needs to report the matter to the Audit Committee or the Board within 2 days of coming to know about the fraud. The MCA requires each of such frauds to be disclosed in the Board's Report. Contents of the auditor's report should include nature of the fraud and a brief description, approximate amount involved in the fraud and potential parties involved. Additionally, the Board's Report should also mention 'Remedial actions taken' in that regard.

The Act has specifically provided a stringent punishment with respect to fraud. Under section 447 of the Companies Act, 2013, any person who is found to be guilty of fraud, shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud.

The Director, Additional Director or Assistant Director of the SFIO on the basis of material in his possession can arrest any person in case he has reason to believe (the reason for such belief to be recorded in writing) that the person is guilty of an offence of corporate fraud covered under section 447 of the Act. In case of foreign companies and government companies, prior written approval of the Central Government for arrest would be required. The SFIO is required to maintain an arrest

register with relevant details of the arrestee, the date and time of arrest, and various other particulars. The provisions of the Code of Criminal procedure, 1973 relating to arrest shall be applicable.

3.2.4 Class Action Suits

On 1 June 2016, the Ministry of Corporate Affairs notified section 245 of the Companies Act, 2013, enlisting the provisions of class action suits in India. In a class action suit, the shareholders of a company collectively institute a suit against the company.

The requirement for provisions of class action suits in India was primarily triggered by the Satyam scam. Satyam shareholders were unsuccessful in claiming damages in India due to the absence of the provision for filing a class action suit under the Companies Act, 1956. On the other hand, the American investors were able to claim their part of damages in the US courts through a class action suit against the company. Accordingly, provisions of class action suit was incorporated to safeguard the interests of shareholders, whenever the company or its directors participate in any fraudulent, unlawful act, or commit an act which is against the interest of the shareholders. The members or the depositors can seek damages or demand suitable action against a director, auditor, expert, advisor or consultant of the company.

In light of the above developments emphasising the need of robust corporate governance, the internal audit function is expected to cover these areas in the internal audit scope depending on the risk based audit plan.

TRANSFORMATION OF THE
INTERNAL AUDIT FUNCTION



Chapter 4 Transformation of the Internal Audit Function

As we witnessed in the earlier chapters, internal audit has a vital role to perform in the current business and governance environment. There is an increase in expectations of various stakeholders leading to increased attention on the overall conduct of Boards, Audit Committees, Internal Audit function and Risk Management function.

Internal audit function aims to achieve operating efficiencies, aid corporate governance and fraud prevention on a day to day basis. Some of the modern-day techniques, approaches, methodologies are narrated below.

4.1 Risk Based Audit Approach

In order to remain within the risk tolerance levels as set by BOD, audit committees constantly assess whether the internal audit function is proactively identifying the ever changing organisational risks and monitoring the mitigating controls.

As a result, it becomes imperative for the internal audit function to follow a Risk Based Audit Approach, provide a value-adding service to the organisation and continuously strive to move up the maturity curve.

Risk based approach entails a systematic process for assessing and integrating professional judgments about probable adverse conditions or events that may affect the achievement of business objectives. Internal audit function needs to identify risks, examine risks, investigate the sources, and put a relative value on each risk to focus on significant risks to ensure adequate risk coverage for meeting stakeholders' expectations.

This needs to be done on a continuous basis for effectiveness of risk management activities. Internal auditors need to develop a comprehensive risk assessment model that factors in the impact and likelihood of the various enterprise risks at inherent as well as residual levels.

Internal auditors have been following a risk based approach in performing audits for quite some years now. However, the speed at which organisations are witnessing

disruptions across people, products, process and technology, the need for internal auditors to remain agile with their risk management approach cannot be over-emphasised.

Internal auditors need to collaborate with other functions within the organisation such as the Enterprise Risk Management and those responsible with management and testing of internal financial controls to ensure adequate alignment of the risk assessment across the organisation. Any change in the risk assessment needs to be factored in the annual internal audit plan so that there is clear focus and prioritisation of the risks that matter.

Figure 4.1 Internal Audit to collaborate with other risk management functions for effective and efficient internal audit.



4.1.1 Business risk assessment and internal audit plan

Risk assessment is one of the most crucial steps in the internal audit lifecycle. Any gaps in risk assessment could lead to an ineffective internal audit coverage. In this context, it is very crucial for the internal auditors to understand the overall business context including factors such as industry pulse, competitive landscape, organisation's strategy and business objectives, end-to-end business cycle and processes, its products, geographical presence, regulatory environment, IT systems landscape, financial statement analysis, existing risk and controls framework, etc.

Based on the above qualitative and quantitative assessment, a risk based internal audit plan is created and depending on the severity of risks assigned to the

individual business processes (e.g. High / Medium / Low), the frequency of internal audit is determined. E.g. high and medium risk areas are covered on an annual basis and low risk areas can be covered once in three years.

Typical processes covered in an internal audit and an illustrative risk-based audit plan (for a manufacturing entity spread across 4 quarters) is given below:

| Process | Risk rating | Q1 | Q2 | Q3 | Q4 |
|---|-------------|----|----|----|----|
| Procure to Pay | H | ☑ | | | |
| Information Technology- General control review | M | ☑ | | | |
| Statutory Compliances | H | ☑ | | | |
| Order to Cash | H | ☑ | | | |
| Inventory Management | M | | ☑ | | |
| Customer Care | M | | ☑ | | |
| Corporate Governance, Risk Management and Internal Financial Controls | H | | ☑ | | |
| Information Security | H | | ☑ | | |
| Supply Chain Management | M | | | ☑ | |
| Advertisement & Marketing | M | | | ☑ | |
| Treasury Management | M | | | ☑ | |
| Capex Management | L | | | ☑ | |
| Financial Statement Closure Process | M | | | | ☑ |
| HR & Payroll | L | | | | ☑ |
| Environment, Health and Safety | H | | | | ☑ |
| Implementation Audits | M | | | | ☑ |

H: High Risk

M: Medium Risk

L: Low Risk

4.1.2 Risk and Control Matrices

Risk & Control Matrices (RCM) or Risk and Control Libraries are key documents used to identify risks, document related controls, and to assess the control design and operating effectiveness for the organisation-wide processes.

A standard RCM typically contains the following details:

- Risk description
- Whether fraud risk (Yes / No)
- Control description (Who does What, When, How, Evidence generated)
- Financial statement assertions
- Type of control (Automated / Manual / IT Dependent)
- Nature of control (Preventive / Detective)
- Frequency of control
- Mapping of the spreadsheets used in control
- Control owner
- Audit steps to be performed
- Conclusions and
- Recommendations

RCMs are typically prepared by the management and owned by the respective process owners for periodic updates. They form the basis for carrying out management testing as part of internal financial controls. Without compromising the independence of an internal audit function, a leading practice followed in large global organisations is internal auditors leveraging the RCMs created by management and customising them for use in their internal audits based on their risk assessment. This helps in reducing process owner "fatigue" from multiple audit related discussions and helps them focus on their core responsibilities.

4.2 Value Added Service

The Chief Audit Executive is not only expected to conserve the existing enterprise value, but also add to the organisational value. Extreme focus on only one of these areas can actually lead to deterioration of audit value.

| Factors leading to conserving the value | Factors leading to value addition |
|--|---|
| Focus on Corporate Governance | Strategic Outlook |
| Compliance to internal policies and procedures | Benchmarking with Industry best practices |
| Following the Audit Charter | Agile Risk Management approach |
| Deploying a risk based approach | Innovative mind-set |
| Coverage of Operational, Financial and Compliance Controls | Anticipation |
| Providing Assurance | Digital Orientation |
| Monitoring of Exceptions | Focus on top / bottom line impact |

The core elements of Value Proposition and how internal auditor can add overall value to an organisation are covered in detail in Chapter 7.

4.3 Moving up the Maturity Curve

Globally, the internal audit function is undergoing a massive transformation in its scope, approach and methodology to meet its overall objectives and the expectations of various stakeholders. This is helping the auditors move up the maturity curve, i.e. from a Basic Internal Audit function to the Internal Audit Function of the Future.

The key parameters to be evaluated to assess the maturity of the internal audit function are summarised in the below table and some of these are elaborated further:

| Parameters | Basic IA Function | IA Function of the Future |
|-------------------|-------------------------------|-----------------------------------|
| Key objectives | Compliance to policies / SOPs | Assurance and Value addition |
| Functional Leader | Head of Internal Audit | CXO level – Chief Audit Executive |
| Role | Fault Finder / Policing | Consultant to Management |

| Parameters | Basic IA Function | IA Function of the Future |
|----------------------------|--|---|
| Outlook / Risk Coverage | Past oriented | Future Oriented / Agile Risk Management |
| Methodology | Checklist driven | Risk Based |
| Independence | Partial | Complete |
| Fraud Coverage | Reactive | Proactive |
| Corporate Governance | By Chance | By Design |
| Digital Intervention | Spreadsheets and macros | CAATs and related tools |
| Working with other teams | Isolated | Collaborative |
| Subject Matter Experts | Nil to limited deployment | Deployed in every audit |
| Awareness | Company knowledge, limited trainings | Industry knowledge, periodic trainings |
| Frequency | At periodic intervals | Continuous monitoring on real time basis |
| Recommendations | Fixes issues, suggests mitigating controls | Fixes issues and suggests more preventive and automated mitigating controls |
| Reporting | Manual, with time lag | Digital, near real time |
| Audit Management | Manual tracking | Internal Audit Management tool |
| Delivery model | 100% on-site audits | Combination of on-site and off-shore audits |
| Feedback from stakeholders | Random | Periodically sought and factored in subsequent audits |
| Team Performance | Limited measurement | Closely tracked against SLAs / KPIs / Audit Charter |



4.3.1 Robust internal audit methodology

An organisation's Internal audit methodology is generally based on globally acceptable SIAs issued by leading Accounting and Auditing Boards. Organisations develop their own internal audit charter aligned to the departmental objectives set by the audit committee of the BOD and adapt a methodology which best suits their business requirements. It is pertinent to note that successful implementation of the adopted methodology is possible when the internal audit team has adequate budgets and the necessary powers (without any limitations) to execute its responsibilities. Hence it is important that the Chief Audit Executive has adequate support and backing from the audit committee to meet its objectives.

Typically, internal audit methodology comprises of five phases, i.e. Initiating, Planning, Executing, Reporting and Closing.



INITIATING

- Independence checks to ensure no conflict of interest of team members
- Engagement acceptance and related risk management and contracting activities

PLANNING

- Assessment of organisational needs, pain points and stakeholder expectations
- Risk-based scoping based on the objectives, business context, qualitative & quantitative assessment
- Internal Audit plan, RCM, data and information request
- Timelines and deliverables agreement with auditees

EXECUTING

- Opening meeting with key stakeholders
- intelligent sample based substantive testing, coupled with Data Analytics
- Root Cause and Impact analysis
- Periodic status updates
- Field work exit meeting

REPORTING

- Draft/Flash reports (if needed), with pragmatic recommendations
- Thorough discussions to reach time bound management action plan
- Quality reviews
- Final report
- Senior Management and Audit Committee reporting

CLOSING






- SLA monitoring
- Project closure checklist
- Engagement closure checklist

A robust methodology would ensure:

- End to end risk coverage
- 360 degrees coverage including operational, financial and compliance aspects of all in-scope processes
- Evaluation of Enterprise Risk Management, Corporate Governance and the Design and Operating Effectiveness of Internal Controls
- Significant emphasis on Data Analytics throughout the Audit Life Cycle
- Deployment of SMEs where needed
- Quality Assurance
- Timely completion of assignment
- Overall Value Addition and Assurance

4.3.2 Internal Audit Delivery Models

Depending upon the organisational culture, geographic spread of operations and specific circumstances faced by the organisations, many corporates are adopting a hybrid internal audit delivery model (combination of on-site and off-shore audits). This helps organisations in optimum utilisation of its resources, leveraging subject matter expertise leading to overall reduction in cost of internal audit.

| Key Activities | Off-shore / On-site possibility |
|--|---|
| Risk Assessment & Audit Scoping and Planning |  |
| Design Assessment |  |
| Data Analytics |  |
| Substantive testing |  |
| Reporting |  |

 On-site  Off-shore

The on-site team is involved in performing critical and strategic activities like risk assessment and scoping, process owner meetings & walk-throughs and senior

management reporting which require on-site presence. On the other hand, the off-shore teams can be based out of a remote shared service centre at a cost effective location, with availability of required skill sets to perform transactional activities such as analytics, remote testing that do not require on-site presence, updates to documentation, testing templates and reporting.

4.3.3 Use of Subject Matter Experts

A key transformational development that is helping the internal audit teams immensely is the hiring or temporary deployment of subject matter experts (SMEs) in the fields such as Accounting, Taxation, Engineering, Supply Chain, IT, Compliance, etc. for effective execution of complex and technical audit areas.

The SMEs are able to deep dive into the technical nuances of the underlying area and identify areas of improvements or any process gaps, which may be beyond the capabilities and skill sets of the regular internal audit team members. How SMEs facilitate in value addition is also touched upon in Chapter 7 on Value Proposition.

4.3.4 Leveraging Digital Tools in performance of Internal Audits

With the advancement of underlying tools and technologies deployed in business operations, over years, internal auditors have moved from auditing around the computer to auditing through the computer. With each passing day, businesses are adopting highly innovative and disruptive technologies such as machine learning, cognitive and artificial intelligence. This is resulting in newer risks which were unheard of before, thereby making the internal audit of such areas highly complex that requires knowledge and training in such areas. Given the importance of the area, this topic is discussed in detail in Chapter 6.

4.4 Conclusion

With each passing day, the parameters of the maturity curve itself are changing dramatically with new parameters either completely replacing or being prioritised over the existing ones. Internal audit functions who will fail to achieve a continuous upward movement on the overall maturity curve and that too at a speed which is at

par with the changing dynamics, will eventually become obsolete and redundant, leaving their organisation exposed to the internal and external world of risks. On the other hand, the internal audit teams which will continue to evolve and transform themselves on the ever changing parameters of maturity curve, will be able to succeed far higher in defending their organisation from the unforeseen risks of the future.

TECHNOLOGY IMPACT AND
CHANGING DYNAMICS OF
INTERNAL AUDIT



5.1 Introduction

The digital and mobility revolution has improved, impacted as well as disrupted business models, processes and efficiencies. The emergence of e-commerce, mobile applications, sophisticated ERPs, block chain solutions, cloud computing, robotic business process automation (RPA), internet of things (IoT), machine learning and artificial intelligence (AI) have added and will add new dimensions to businesses. The internal audit function needs to re-orient itself to meet the requirements in this digital era as well as improve its own approach and methodology.

5.2 Some key questions around Information Technology (IT) risk management and internal audit that organisations face in today's disruptive environment

- Are the controls and Segregation of Duties (SoDs) mapped correctly in your IT/ERP systems? What are the over-rides and the mechanisms for audit trails of such over-rides?
- Does your audit plan identify key IT risks that have direct significant impact on the organisation?
- Is IT audit part of your internal audit plan?
- Have you identified opportunities to reduce manual controls by increasing automated controls?
- Have you identified areas in your internal audit plan where data analytics can be used for the audit of complete or larger set of data set rather than sample based approach?
- Have you assessed the business, financial, legal and reputational risks associated with data leakage or cyber frauds? Have you effective control and audit mechanisms in place to counter the same?

- Have you ascertained applicable data privacy regulations and put in place the mechanism required to conform to the same? Are the same covered in the internal audit and/or IT systems audit?
- Have you identified the laws requiring digital filings and reporting? Are their effective controls for the digital authorization of the filings (DSCs), review of compliances, receipt and adherence to any on-line notices/proceedings, etc.?
- Have you identified areas in your audit plan where technology can be used to evaluate the effectiveness of controls against the key risks?
- Does your Internal Audit team have sufficient IT competencies to evaluate the effectiveness of controls?
- Do you have a program/framework established to ensure the above aspects are verified on a continual basis?

5.3 Information Technology in Internal Audit – A Key Differentiator

- Internal audits are designed to evaluate the effectiveness of organisation's internal controls by first gathering information about how a unit operates, identifying points at which errors or inefficiencies are possible and then identifying system controls which are designed to prevent / detect such occurrences. Then, the application and performance of those controls are tested to assess how well they work. Managers must consistently evaluate controls in their department's operations by following the same process.
- IT provides most of the information needed for auditing. In order to be effective, auditors must use IT as an auditing tool, audit automated systems and data, to understand the business purposes for the systems, and understand the environment in which the systems operate.
- The other important uses of IT by auditors are in audit administration. By seeking new use for computers and communications, auditors improve their

ability to review systems and information and manage their activities more effectively. Automated tools helps in increasing the individual productivity. By recognising the importance of emerging environment and requirement to perform audit task effectively, auditors must recognise the key reasons to use audit tools and software.

- Some of the examples below demonstrate the need for an effective internal audit function leveraging technology platform.

5.4 Key IT considerations for Internal Audit

- Information Security**

| Information Security | Key IT Internal Audit Considerations |
|--|---|
| Information security program assessment: Evaluates the organisation's information security program, including strategy, awareness & training, vulnerability assessments, predictive threat models, monitoring, detection and response, technologies & reporting. | <ul style="list-style-type: none"> How comprehensive is the existing information security program? Is information security embedded within the organisation, or is it an "IT only" responsibility? How well does the organisation self-assess threats and mitigate the threats? How well the organisation find the vulnerabilities and the solution for that? |
| Threat and vulnerability management program assessment: Evaluates the organisation's Threat and Vulnerability Management (TVM) program including threat intelligence, vulnerability identification, detection, remediation, response, and countermeasure planning. | <ul style="list-style-type: none"> How comprehensive is the existing TVM program? Is the TVM program aligned with business strategy and therisk appetite of the organisation? Are the components of TVM integrated with one another, as well as with other security and IT functions? |

| Information Security | Key IT Internal Audit Considerations |
|----------------------|--|
| | <ul style="list-style-type: none"> • Do processes exist to make sure identified issues are appropriately addressed and remediation is effective? • What counter measures have been planned for the threats with the TVM? |

■ **Business Continuity Management**

| Business Continuity Management | Key IT Internal Audit Considerations |
|---|---|
| <p>Business continuity program integration and governance audit: Evaluates the organisation's overall business continuity plan, including program governance, policies, risk assessments, business impact analysis, vendor/third-party assessment, strategy/plan, testing, maintenance, change management and training/awareness.</p> | <ul style="list-style-type: none"> • Does a holistic business continuity plan exist for the organisation? • How does the plan compare to leading practice? • Is the plan tested? • What impacts the plan and how the plan will affect the business? |
| <p>Disaster recovery audit: Assesses IT's ability to effectively recover the systems and resume their regular performance in an event of disruption or disaster.</p> | <ul style="list-style-type: none"> • Are disaster recovery plans aligned with broader business continuity plans? • Do testing efforts provide confidence that systems can be effectively recovered? • Are all critical systems included? Are critical systems defined? |
| <p>Crisis management audit: Reviews the organisation's crisis management plans, including overall strategy/plan, asset protection, employee safety,</p> | <ul style="list-style-type: none"> • Are crisis management plans aligned with broader business continuity plans? • Are plans comprehensive and do they |

| Business Continuity Management | Key IT Internal Audit Considerations |
|--|---|
| communication methods, public relations, testing, maintenance, change management and training/awareness. | involve the right corporate functions? <ul style="list-style-type: none"> • Are plans well communicated? |

■ **Mobile Security**

| Mobile Security | Key IT Internal Audit Considerations |
|--|---|
| Mobile device configuration review: Identifies risks in mobile device settings and vulnerabilities in the current implementation. This audit includes an evaluation of trusted clients, supporting network architecture, policy implementation, management of stolen / lost devices and vulnerability identification through network accessibility and policy configuration. | <ul style="list-style-type: none"> • How has the organisation implemented "bring your own device" (BYOD)? • Are the right policies/mobile strategies in place? • Are mobile devices managed in a consistent manner? • Are configuration settings secure and enforced through policy? • How do we manage lost and stolen devices? • What vulnerabilities exist, and how do we manage them? |
| Mobile application black box assessment: Performs audit using different front-end testing strategies: scan for vulnerabilities using various tools, and manually verify the scan results. Attempts to exploit the vulnerabilities identified in mobile web apps. | <ul style="list-style-type: none"> • What vulnerabilities can be successfully exploited? • How do we respond when exploited, and do we know an intrusion has occurred? |
| Mobile application grey box assessment: Combines traditional source code reviews (white box testing) with front-end (black box) testing techniques to identify critical | <ul style="list-style-type: none"> • How sound is the code associated with the mobile applications used within the organisation? • What vulnerabilities can be exploited within the code? |

| Mobile Security | Key IT Internal Audit Considerations |
|---|---|
| <p>areas of functionality and for symptoms of common poor coding practices. Each of these 'hot spots' in the code should be linked to the live instance of the application where manual exploiting techniques can verify the existence of a security vulnerability relations, testing, maintenance, change management and training/awareness.</p> | <ul style="list-style-type: none"> • Whether OWASP top 10 vulnerabilities are present in the code? |
| <p>Device security configuration</p> | <ul style="list-style-type: none"> • Have your IT servers, infrastructure securely hardened? • Are the security patched updated appropriately? • Do you follow leading industry practices to secure systems? |

■ **Cloud Security**

| Cloud Security | Key IT Internal Audit Considerations |
|--|--|
| <ul style="list-style-type: none"> • Cloud strategy and governance audit: <ul style="list-style-type: none"> - Evaluates the organisation's strategy for utilising cloud technologies. Determines whether appropriate policies and controls have been developed to support the deployment of the strategy. - Evaluates alignment of the strategy to overall company objectives and the level of preparedness to adopt within the organisation. | <ul style="list-style-type: none"> • Are there supporting policies to follow when using a cloud provider? Are policies integrated with legal, procurement & IT policies? How to make the organisation to adopt the changes? |

| Cloud Security | Key IT Internal Audit Considerations |
|---|---|
| <ul style="list-style-type: none"> • Cloud security and privacy review: <ul style="list-style-type: none"> – Assesses the information security practices and procedures of the cloud provider. This can be a review of their SOC 1, 2 and/or 3 report(s), review of their security SLAs and/or an on-site vendor audit. – Determines whether IT management has worked to negotiate security requirements into their contract with the provider. – Reviews procedures for periodic security assessments of the cloud provider(s) and determine what internal security measures have been adopted to protect company information and data. | <ul style="list-style-type: none"> • Does your organisation have secure authentication protocols for users working in the cloud? • Have the right safeguards been contractually established with the provider? |
| <p>Cloud provider service review: Assesses the ability of the cloud provider to meet the agreed-upon Service Level Agreements (SLAs) in the contract. Areas of consideration should include technology, legal, governance, compliance, security and privacy. In addition, internal audit should assess what contingency plans exist in case of failure, liability agreements, extended support, and the inclusion of other terms and conditions as part of the service contracts, as well as availability, incident, and capacity management and scalability.</p> | <ul style="list-style-type: none"> • What SLAs are in place for uptime, issue management and overall service? • Has the cloud provider been meeting or exceeding the SLAs? • What issues have there been? • Does the organisation have an inventory of uses of external cloud service providers, sponsored both within IT and directly by the business units? |

■ **Social Media Risk Management**

| Social Media Risk Management | Key IT Internal Audit Considerations |
|---|--|
| <p>Social media risk assessment: Collaborates with the IT organisation to assess the social media activities that would create the highest level of risk to the organisation. Evaluates the threats to the organisation's information security through the use of social media. This audit may be combined with a social media governance audit to then confirm policies have been designed to address the highest risks to the organisation.</p> | <ul style="list-style-type: none"> • Has the organisation identified what risks exist related to social media? • How well are the identified risks managed or mitigated? • Does the organisation periodically conduct a social media audit? |
| <p>Social media governance audit: Evaluates the design of policies and procedures in place to manage social media within the organisation. Reviews policies and procedures against leading practices.</p> | <ul style="list-style-type: none"> • Does a governance process exist for social media within the organisation? • How well are policies related to social media known amongst employees? |
| <p>Social media activities audit: Audits the social media activities of the organisation and its employees against the policies and procedures in place. Identifies new risks and assist in developing policies and controls to address the risks.</p> | <ul style="list-style-type: none"> • Are social media activities aligned to policy? • What corrective actions need to be put in place given activity? • How does existing activity affect brand and reputation? |

■ **Segregation of Duties and Identity Access Management (SoD & IAM)**

| SoD & IAM | Key IT Internal Audit Considerations |
|---|---|
| <p>Systematic segregation of duties review audit: Evaluates the process and controls IT has in place to effectively manage segregation of</p> | <ul style="list-style-type: none"> • How does IT work with the business to identify cross application segregation of duties issues? • Are business personnel adequately |

| SoD & IAM | Key IT Internal Audit Considerations |
|---|---|
| <p>duties. Performs an assessment to determine where segregation of duties conflicts exist and compare to known conflicts communicated by IT. Evaluates the controls in place to manage risk where conflicts exist.</p> | <p>informed of the ERP roles well enough to perform user access reviews?</p> <ul style="list-style-type: none"> • While compensating controls identified for SoD conflicts may detect financial misstatement, would they truly detect fraud? |
| <p>Role design audit: Evaluates the design of roles within ERPs and other applications to determine whether inherent SoD issues are embedded within the roles. Provides role design, role clean-up or role redesign advisory assistance and pre- and post-implementation audits to solve identified SoD issues.</p> | <ul style="list-style-type: none"> • Does the organisation design roles in a way that creates inherent SoD issues? • Do business users understand the access being assigned to roles they are assigned ownership of? |
| <p>Segregation of duties remediation audit: Follows up on previously identified external and internal audit findings around SoD conflicts.</p> | <ul style="list-style-type: none"> • Does the organisation take appropriate action when SoD conflicts are identified? • Have we proactively addressed SoD issues to prevent year-end audit issues? |
| <p>IAM/GRC technology assessment: Evaluates how IAM or GRC software is currently used, or could be used, to improve SoD controls and processes.</p> | <ul style="list-style-type: none"> • Is IAM or GRC software currently used effectively to manage SoD risk? • What software could be utilised to improve our level of SoD control, and what are our business requirements? |

■ **Data Loss Prevention (DLP) and Privacy**

| Data Loss Prevention and Privacy | Key IT Internal Audit Considerations |
|--|--|
| <p>Data governance and classification audit: Evaluates the processes management has put in place to classify data and develop plans to protect the</p> | <ul style="list-style-type: none"> • What sensitive data do we hold – what is our most important data? • Where does our sensitive data reside, both internally and with third parties? |

| Data Loss Prevention and Privacy | Key IT Internal Audit Considerations |
|---|--|
| data based on the classification | <ul style="list-style-type: none"> • Where is our data going? |
| <p>DLP control review: Audits the controls in place to manage privacy and data in motion, in use and at rest. Considers the following scope areas: Perimeter security, network monitoring, use of instant messaging, privileged user monitoring, data sanitation, data redaction, export/save control, endpoint security, physical media control, disposal and destruction, and mobile device protection.</p> | <ul style="list-style-type: none"> • What controls do we have in place to protect data? • How well do these controls operate? • Where do our vulnerabilities exist, and what must be done to manage these gaps? |
| <p>Privacy regulation audit: Evaluates the privacy regulations that affect the organisation, and assess management's response to these regulations through policy development, awareness and control procedures.</p> | <ul style="list-style-type: none"> • How well do we understand the privacy regulations that affect our global business? For example, HIPAA is potentially a risk to all organisations, not just health care providers or payers or GDPR is applicable to organizations even if they do not have operations in the EU?. • Do we update and communicate policies in a timely manner? • Do users follow control procedures to address regulations? |

■ **Machine Learning**

| Machine Learning | Key IT Internal Audit Considerations |
|--|---|
| <p>Machine learning technology helps in finding the unstructured data, which include the emails and the social media</p> | <ul style="list-style-type: none"> • What controls do we have in place to protect unstructured data e.g. emails? |

| Machine Learning | Key IT Internal Audit Considerations |
|---|--|
| posts and review them. | <ul style="list-style-type: none"> • Is there any important data leaking out through social media? • Where is our data going? |
| Machine learning may be applied to help with the classification of transactions. Inductive reasoning could be applied to the source data of historical transactions to help “predict” the classification of additional transactions as they are recorded. | <ul style="list-style-type: none"> • What is the historical transaction pattern? • How the transactions are been classified? • What are the controls to protect the historical transaction data? |
| Machine learning has the ability of the computer to recognize and apply patterns, derive its own algorithms based on those patterns, and refine those algorithms based on feedback. | <ul style="list-style-type: none"> • What is the pattern of data been processed? • What type of algorithms in place for analysis so it meet the requirements? • Does any feedback mechanism been carried? |

■ **Block Chain**

| Block Chain | Key IT Internal Audit Considerations |
|---|--|
| In a blockchain system, the ledger is replicated in a large number of identical databases, each hosted and maintained by an interested party. When changes are entered in one copy, all the other copies are updated simultaneously. So as the transactions occur, records of values and assets exchanged are permanently entered in all ledgers. | <ul style="list-style-type: none"> • What Existing policies and procedures will need to be updated to accommodate blockchain protocols and integrate blockchain transactions into legacy systems? |
| Blockchain technology helps to test the whole population of transactions within the period under observation. This extensive coverage drastically | <ul style="list-style-type: none"> • What type of data is processed? • Is the data structured or unstructured? • What controls do we have in place to |

| Block Chain | Key IT Internal Audit Considerations |
|--|--|
| improves the level of assurance gained in affected audit engagements. | protect data? |
| Blockchain Uses the encryption technology which help to secure the data. | <ul style="list-style-type: none"> • What Credential and key management is crucial to protect the digital assets stored on the blockchain? • Who will have access to the data and encryption keys? |

■ **Robotics Process Automation**

| Robotics Process Automation | Key IT Internal Audit Considerations |
|--|---|
| RPA is configurable software, that works on the existing IT infrastructure, pulling data, performing algorithms and creating reports. It uses business rules, can be configured to perform a variety of processes enabling multi-use robots, and variability as your business needs change. | <ul style="list-style-type: none"> • Does the present infrastructure support RPA? • What are the Data Governance and Controls Standards in the context of RPA? • What Privacy and Data Protection the organisation follows in the context of RPA? • Have optimised processes before we automated? |
| RPA offers broader spectrum of internal and external application integration in risk. It helps to create document repositories and connections to existing governance, risk and control (GRC) platforms that are linked to processes, risks and controls to demonstrate framework adherence and evidence traceability. | <ul style="list-style-type: none"> • What level of control implemented to organisation on the integration of application? • Do business users understand the access being assigned to roles they are assigned ownership of? |

5.5 Conclusion

Understanding the risks in the digital era and mapping out a strategy to ensure that IT controls are in place is a crucial step for businesses where internal audit can play a significant role. The effectiveness of internal audit itself can be enhanced with the use of technology and tools.

DATA ANALYTICS – EFFECTIVE
TOOL FOR INTERNAL AUDITORS



Audit transformation through innovation and technology

By embedding analytics in audit process, internal audit can support in navigating complex business scenarios covering varied business areas during the course of audit. This new approach to integrate analytics into internal audit is referred as the 'Data - driven audit analytics.'

6.1 Data-driven Audit Analytics: A Multidisciplinary Approach

Data driven audit analytics is an analytical process by which insights are extracted from operational, financial, and other forms of electronic data internal or external to the organisation.

These insights can be real-time, historical, or predictive and can also be:

- **Risk focused** (e.g., controls effectiveness, fraud, abuse, policy/regulatory non-compliance) or
- **Performance focused** (e.g., increased sales, decreased costs, improved profitability)

6.1.1 Data Analytics: 'What & Why'

It enables:

- Optimal decision making
- Increased business assurance levels
- Elimination of "Grey Areas"

It answers:

- **Historical Perspective** – What happened, how often & where
- **Current Perspective** – Why it happened & what actions need to be taken
- **Future Perspective** – "What If" scenarios

While technology can be used to achieve the same level of assurance more efficiently at a lower cost, a greater benefit derived is by achieving a higher level of assurance at a similar cost – which ultimately results in better audit quality for clients and investors and reduces audit risk and liability.

The success of the analytics embedded internal audit translates into the financial benefits to an organisation by giving an opportunity to tighten the controls thereby minimising the risks.

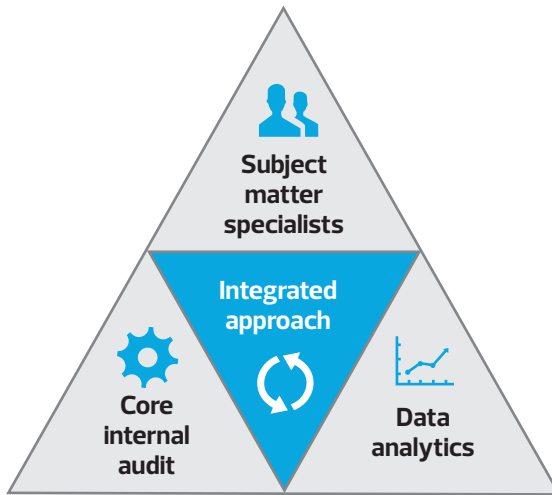


Figure 6.1 Integrated approach to Data Driven Audit Analytics

6.1.2 Benefits of a Data-driven Approach

The benefits of data driven auditing can be summarised into four simple statements:

- **Enhanced focus on critical risks**

Improving the access to data and developing key insights before the fieldwork commences, making connections and comparing performance & key benchmarks between products, processes and business units means

the auditor can focus only on what is of utmost importance and avoid merely confirming the obvious; or assessing transaction risks in real time.

- **Do more with less**

Connecting the auditor directly to the process through the data with risk analytics and data visualisation allows analytics to drive a more focused audit, while still testing 100 percent of the population and moving to automated scheduled Script run over manual audit saves time and money.

- **Better Audit Productivity**

Combining data from inside and outside the organisation, adding new richness and granularity to insights and also the understanding of risk. Benchmarks, comparative analysis, and trending enhance on-the-job learning and development while delivering a more impactful result to business stakeholders.

- **Making use of technology: an imperative part of audit process**

Providing a rich combination of data science disciplines and using a new generation of technologies enhances, automates and continuously improves the audit process, reporting and service delivery.

6.2 Implementing Analytics-enabled Function

A simple three-stage approach for implementing the analytics function as an integral part of the audit process:

- **Assessment:** Analyse current analytics capabilities both within IA and across the business and rapidly develop proof of concepts to identify challenges and opportunities.
- **Roadmap:** Create a long-term strategy and vision for analytics; scope and prioritise projects to achieve this.

- **Deliver and monitor:** Initiate the program, deliver the roadmap, and monitor your implementation successes against key performance indicators.

Becoming analytics-enabled relies on the fundamental building blocks of people, data, process and technology, all being informed by an analytics strategy.

This enables the embedding of analytics into the audit lifecycle, focusing on the right risks at the right time while aligning the analytics to the IA strategy and value drivers of the business.

While few organisations are on the cutting edge right now, insights-driven auditing will become pervasive among leading companies by 2020.

While we are making significant progress of big data and analytics in the audit and are beginning to see the benefits, we recognise that this is a journey.

The transition to this future would not happen overnight. It is a massive leap to go from traditional audit approaches to one which fully integrates big data and analytics in a seamless manner.

Audit analytics can be used at every single stage of audit viz:

| | |
|--|--|
| Risk assessment Either Ad-hoc testing or as a part of the continuous risk monitoring process. | Planning Analytics can drive more targeted auditing focusing on segments with highest risks. |
| Fieldwork Analytics can provide a higher degree of assurance and perform testing more efficiently. | Reporting Auditors can provide more insightful actionable outcomes helping quantify risks identifying root causes. |

6.2.1 Key Activities in the Audit Analytics Cycle

■ Defying the Problem Statement

- Identify the subject area and the detailed audit objective(s) to be developed. (E.g. Within the Accounts payable domain the controls for payment processing to the vendors needs to be evaluated)
- Plan, prioritize and document the tests (in plain language) Deliverables in the Analytic Requirements Document

■ Data Import

- Identify systems, data storage, data owners, data format (specs) and file requirements
- Verify completeness and accuracy of data (validate)
- Identify any gaps in required data (cleanse if needed)

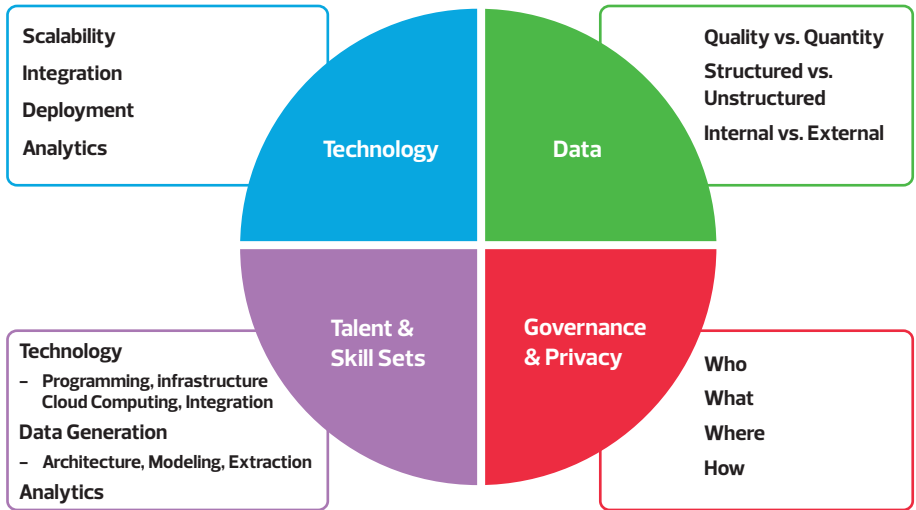
■ Building the Analytics Script

- Develop test scripts and queries
- Execute test scripts and improvise the code

■ Exception Reporting

- Interpret and analyse the results generated out of the test scripts
- Detailed analysis of data sets and outputs against the analytic objectives by verifying the results from the actual data
- Interpret and report results in the form of Exception Report

Keys Aspects for Implementing Analytics



6.2.2 Transformation Attained with Data Analytics

Some of the advantages of deploying Data Analytics are as under:

- Timely detection of Red flags
- Maintains an audit trail
- Increased assurance to the management
- Automation of the audit process thereby saving time
- Data analytics help in trending of transactions
- Introducing the control culture (you are being watched)
- Capable to analyse huge amount of data volumes
- Addressing the leaking controls so as to mitigate risks

- Effectively highlight “Opportunities for Improvement”
- Capability to connect with multiple databases and multiple platforms.
- Increased audit efficiency by automating transaction testing for key risk areas
- Improves audit coverage by covering 100% data rather than relying on sample data
- Improves audit consistency by applying standard audit analytic techniques across projects and over time
- Timely detection of questionable transactions – Proactive approach rather than being reactive
- Enables auditors to implement analytics as an objective, automated and consistent way to measure and improve business controls

6.2.3 Practical Applications of Data Analytics

Some examples of data analytics that can be performed across various processes are as follows:

- **Record to Report Cycle**
 - General Ledger analysis
 - Journal Entries by unauthorised users
 - Duplicate JEs (same account/amount, same JE number/amount)
 - Split JEs (single JE/multiple accounts, multiple JEs/single account)
 - Segregation of duties (park vs. post, post vs. create account)
 - Analysis of entries in dormant accounts

- Suspicious keyword in Journal Entry description
- Compare summaries by major account in high / low order
- Identify dormant accounts with activity or change in address

- **Purchase to Pay Cycle**

- Validation of Critical data fields (Vendor master, Requisition, Purchase order)
- Analysis of Split requisitions and Purchase Orders
- Checking of Stale requisitions and Purchase Orders
- Segregation of duties (Maker Checker validation)
- Purchase Order date after Invoice date
- Invoice number sequence validation
- Goods received quantity vs. Invoice quantity
- Review changes to the vendor master file
- Employee and vendor matches by name and by address
- Find invoice payments issued on non-business days (Saturdays and Sundays)
- Identify multiple invoices at or just under approval cut-off levels
- Vendor Master analysis – Duplicate vendors (by name, address, bank account number)
- Duplicate purchases (same vendor same invoice number, same amount same GL account)

- Isolate Vendor Unit price variances by product over time
 - Reconcile selected vendor payables posted against POs
 - Summarise large invoices without POs by amount, vendor , service type, etc.
 - Stratify vendor balances, check amounts, invoice amounts, PO amounts, etc., for unusual trends or exceptions

- **Payroll**

- Payroll Master file validation
- Employee status not matching the termination date
- Reconciliation of hours worked vs. hours paid
- Employee start date after pay check date
- Invalid pay rates (actual/calculated vs. master file)
- Employee Master validation (same name, same bank account or address etc.)
- Compare and summarise costs for special pay, overtime, premium etc.
- Job record frequent unauthorised alteration (data corrections not using effective date)
- Compare time card rates and pay to payroll to indicate variances
- Verification of commission paid to employees

- **Travel and Entertainment Expenses**

- Even/small dollar amount transactions

- Potential duplicate reimbursements
- Detect suspicious purchases
- Identify both one-time and chronic offenders
- Analysis of declined and disputed transactions
- Analysis of weekend and holiday transactions
- Evaluate suspicious keyword in the transaction description
- Analysis of spending limits on transactions (lavish hotel stays, dinners, etc.)
- Review inappropriate spending in designated categories based on merchant category codes
- **Stock & Inventory Control**
 - Identify obsolete inventory by turnover analysis
 - Analyse the difference between standard costs and actual costs
 - Identify items with yearly volume under the prescribed threshold limits
 - Match stock receipts with vendor ledger and report variances
 - Report on products in order of profitability (low-high, high-low)
 - Report analysing usage & ordering quantity to improve the turnover
 - Summarise products by group, location, type, etc.
 - Evaluate Product Pricing and impact on turnover for changes in product pricing

- Verify product reordering volumes by item, warehousing, vendor, period, etc.

- **Order to Cash**

- Customer Master validation of critical data fields (customer name, Bank account, address)
- Analysis of credit limits versus total value of orders processed
- Validate unauthorised / excessive commission payouts
- Compare delivered quantity vs sales order quantity
- Report shipments/ sales orders/ price changes by unauthorised employee
- Identify high value credit notes, balances and Invoices
- Summarise payment by clients based on sales, product, region etc.
- Report shipments without a Sales order
- Comparison of periods for unusual trends
- Segregation of duties (order entry vs. customer master, order entry vs. product master)

6.3 Team composition for implementing Data Analytics

- **Audit Management and Staff**

- Provides comprehensive understanding of the audit objectives
- Identifies opportunities to introduce data analytics into the audit process.
- Drives demand through personal insights and relationships.

- Keeps focus on solving audit related issues
- **Data Analytics Subject Matter Expert**
 - Experienced auditor with a knack for analysis
 - May have knowledge of advanced statistical topics and modeling
 - Excellent problem solving skills key roles and responsibilities within internal audit
 - Proficient in use of DA tools and is able to design queries and manipulate data easily
- **Data Specialist**
 - Strong programming and coding proficiency
 - Has been a database administrator or systems analyst
 - Has spent time as developer and has built applications
 - Expertise in core IT related functions in querying, data extraction, cleansing, and manipulation

6.4 Conclusion

With the appropriate application of Data Analytics across the internal audit cycle, Internal Auditors will be able to transform themselves from a traditional, judgement based, sample driven, manual intensive and reactive audit approach to one that is risk focused, continuous and real time and most importantly data centric.

INTERNAL AUDIT VALUE
PROPOSITION AND VALUE DELIVERY



As seen in earlier chapters, the demands on internal audit have increased significantly in recent years as technology has advanced, regulation has become more rigorous, risks have emerged, and companies have sought more business insights from internal audit teams. One pertinent question for all stakeholders' is "What should the senior management expect from internal auditing?" The very definition of internal audit states that it is "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations". Let us dwell into what is value proposition.

7.1 Core Elements of Value Proposition

- A value proposition is a statement which identifies clear, measurable and demonstrable benefits that users get when availing a particular service. It should convince the users that this service is better than others in the market. This proposition can lead to a competitive advantage when the users select a particular service provider over others because they receive greater value.
- Value proposition is based on core elements like getting proper insights, objectivity in assessment and providing assurance. In order to deliver a value proposition, internal auditor needs to objectively assess the function by gaining proper insight into the process. He / she needs to comment on the effectiveness of governance, robustness of risk management culture, and maturity of internal control processes.
- Internal Auditor's value will be measured by his ability to drive positive change and improvement within the organisation with the help of the observations noted and his recommendations.
- Creating and delivering value proposition is a significant issue that we need to consider in planning strategies. Value propositions vary across industries and across different segments within an industry.

- Client value should also drive investment and service decisions, because clients perceive value on the benefits of the service they receive. Consequently, as the environment changes, and the client experience and their desires change, the value they seek changes.

7.2 Internal Auditing under each of the core element provides:

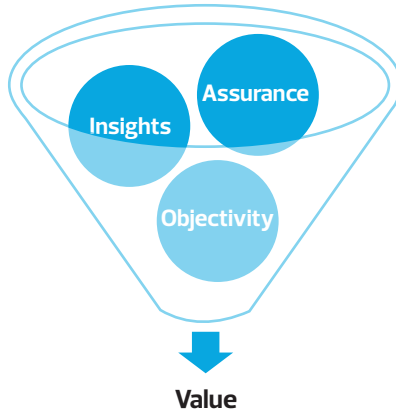


Figure 7.1 Delivering Value through Assurance, Insights and Objectivity

- Assurance is a part of corporate governance in which accurate and current information is provided to stakeholders about the efficiency and effectiveness of its policies, procedures and operations as well as its compliance status with statutory regulations. Under assurance, the governance, risk and controls are evaluated.
- Insight is the quality to have a clear understanding of complicated problem or situation, deep dive into the matter to facilitate resolution. Insight for improving controls, processes, procedures, performance, risk management, for reducing expenses, enhancing revenues, and improving profits. Under insight, the role and approach is more of that of a catalyst, doing specific analysis and a detailed assessment is carried out.
- Objectivity is to reduce or eliminate biases, prejudices, or subjective

evaluations by relying on verifiable data. Reliance is placed on verifiable evidence (such as delivery notes, invoices, orders, physical counts, paper or electronic trail) in the measurement of financial results. Objectivity makes it possible to compare financial statements of different organisations with an assurance of reliability and uniformity. Under Objectivity, the Integrity, Accountability and Independence are evaluated.

7.3 Value Proposition through Governance

- Governance is the way the rules, norms and actions are structured, sustained, regulated and held accountable. The degree of formality depends on the internal rules of a given organisation and, externally, with its business partners. Governance may take many forms, driven by many different motivations and with many different results.
- Compliance requirements have risen dramatically over the past few years as legislators attempt to help businesses avoid issues that lead to financial crisis. The audit also focusses on strategic, operational and financial risk. Audit function serves as a governance control.
- It performs a crucial role by strengthening the organisation's overall system of control and conducting assurance reviews of critical controls intended to address entity-level, industry and business risk.
- These reviews provide management, Board of Directors, External Auditors, Audit Committees an assurance that key controls within the organisation are designed appropriately, operating effectively and efficiently and functioning to protect stakeholders. It may not be possible for auditors to quantify the assurance in monetary terms, but definitely constitutes value added service.

7.4 Deliver Value through Subject Matter Experts

- In an internal audit team, there are people with diverse skills, educational backgrounds and expertise. The task is to use the knowledge of the

business to help and facilitate the management to achieve its business objectives and making recommendations that are practical and transformative.

- An appropriate mix of core internal audit team members and subject matter specialists (those with significant business acumen) facilitates in meeting the stakeholder expectations. Further, the continual learning and development model improves the internal audit knowledge of the business and related risks.

7.5 Unleash Value through Technology

- In chapter 6, the value delivered through technology was covered in detail. We saw how the use of technology to perform data analytics allows alignment with business areas together with greater assurance on testing of results through automation.
- Continuous audit techniques can be leveraged to enhance the audit coverage, provide early warning or risk indicators and improved governance.
- Rising use of data analytics is an opportunity for internal audit department to improve efficiency, reduce costs, increase accuracy and expand the testing universe.
- By pinpointing likely risk areas for testing, internal audit personnel can be deployed more strategically, leaving room for additional testing areas. Advanced Data analytics tools helps the organisations improve compliance through the ability to anticipate upcoming risks and make appropriate decisions on mitigating such risks.

7.6 Value through Blue Print of Audit Methodology, Approach and Geographic Spread

- For a value added delivery, audit methodology needs to be standardised and simplified.
- The audit plan is changed to incorporate the changes in the organisation and

external business environment. Appropriate time and efforts are involved in assessing the risk associated with the enterprise and focus on areas that matter.

- Through use of both internal staff and network associates at a varying staff level, use of standard risk based audit checklist, leveraging team's geographic presence, audits are concluded keeping value in delivery in mind.
- Productivity is measured and managed on recurring basis to ensure cost effectiveness in delivery. For example, reviews where on-site presence is not required, internal audit teams can deploy desk top reviews or remote site audits to enable cost effectiveness.

7.7 Value Index Benchmark

- The performance of internal audit function should be measured periodically (ideally annually) to ensure that it meets with the organisational and audit objectives set out in the beginning.
- Each organisation should therefore devise an objective methodology for assessing contribution made by the internal audit, both in financial as well as in non-financial terms. This should be then compared with the cost of internal audit function to arrive at cost benefit analysis and assessing its contribution.
- Value addition effectively means to demonstrate clear savings which are directly attributable to the conduct of audit. This should be mutually accepted and clearly established in the report in an unambiguous manner. Objective of the reporting is to highlight into the report the Savings that can be in the form of:
 - Confirmed / Probable value gain
 - Confirmed / Probable losses avoided
 - Opportunity gain
 - Cost reduction possibilities

- In case of outsourced audit function, it is relatively easier to arrive at cost of internal audit. However, for the in-house audit function costs such as direct cost of manpower, indirect costs and administrative costs, time spent by senior management in review, infrastructure costs, etc. should be considered.
- While it is difficult to measure contribution in non-financial terms, some guidelines should be made considering aspects such as mitigation of risks, avoiding non value add activities, possibilities of automation against manual work, improvement in customer satisfaction and trust, etc. However, in the long run, such intangible contributions always get converted into tangible and measurable gains by the organisations.
- Based on the savings achieved vis-à-vis costs of internal audit, a factor can be established which should serve as a good guide to assess performance and contribution made by the internal audit.
- Some organisations have also instituted a system of internal surveys based on the express perception of auditee functions on the internal audit. A set of questions as to tangible and intangible benefits is devised and each auditee function covered by the internal audit is required to provide its feedback, based on which a scoring methodology is arrived at. This is then combined at organisational level to assess the overall performance of the internal audit. However, due to the inherent problems such as organisational and inter functional dynamics, this method has its own limitations and therefore not very popular method to assess internal audit performance.

7.8 Some of the other parameters of gauging the value additions are:

- Environmental impact of the recommendation suggested and sustainability in long term – E.g. for a factory audit, commenting on the type of fuel used to run boiler operations, the same is operated through High Speed Diesel (HSD), Furnace Oil (FO), briquettes, etc. While briquettes may be the most cost efficient in terms of cost savings, but it also has an environmental

impact. Accordingly, it is not always cost savings which is centre point but also environmental impact which is taken into consideration.

- Process improvement leading to less paperwork and improved efficiency. E.g. Formulating SOPs and processes involve keeping more and more trails. In the process, it becomes sometimes dilemma between excessive controls v/s. reasonable controls which leads to more paperwork. The focus should be to move towards less paperwork, system based track which will in turn improve efficiency.
- Comprehensively assessing the Risk and Control effectiveness
- Establishing and reporting key performance parameters
- Internal and external quality assessment
- Compliance measures with IA standards, other standards and organisation's audit plan

7.9 Conclusion

The key role of internal audit function, irrespective of organisation's depth and breadth is to create and add value to its business activities. The internal audit function which can achieve these objectives can partner the growth of the organisations in true sense.

RSM India



Mumbai

13th Floor, Bakhtawar
229, Nariman Point
Mumbai – 400 021

3rd Floor, A Wing,
Technopolis Knowledge Park
Mahakali Caves Road, Andheri (E)
Mumbai – 400 093

201, Shree Padmini
Teli Galli Junction
Andheri (E), Mumbai – 400 069

New Delhi – NCR

2nd Floor, Tower-B
B-37, Sector-1
Noida – 201301

Chennai

Apex Towers, 2nd Floor, No.54
II Main Road, R. A. Puram
Chennai – 600 028

1A, Chamiers Apartments
62/121, Chamiers Road
R. A. Puram, Chennai – 600 028

Kolkata

A-6, 12th Floor
Chatterjee International Centre
33A, Jawaharlal Nehru Road
Kolkata – 700 071

Bengaluru

3rd Floor, B Wing
Jubilee Building, 45, Museum
Road, Bengaluru – 560 025

Surat

DTA-2, G-02 to G-05 Plot
Gujarat Hira Bourse
Ichhapore-2
Surat – 394 510

T-720, Belgium Tower
Opp. Linear Bus Stop
Ring Road, Surat – 395 002

B/604-605, Tirupati Plaza
Athwa Gate, Nanpura
Surat – 395 001

Hyderabad

217, Maruthi Corporate Point
Swapnalok Complex
92, Sarojini Devi Road
Secunderabad – 500 003

Ahmedabad

B-504, Narnarayan Complex
Navrangpura
Ahmedabad – 380 009

Pune

102, 1st Floor
Shree Residency
Baner Balewadi Road
Balewadi, Pune – 411 045

Gandhidham

Divyasatika, Plot No. 41
Ward 10-A, Gurukul
Gandhidham – 370 201

Jaipur

346, 3rd Floor
Ganpati Plaza, M.I. Road
Jaipur – 302 001

For further information please contact:

RSM Astute Consulting Pvt. Ltd.

13th Floor, Bakhtawar, 229, Nariman Point, Mumbai – 400 021.

T: (91–22) 6108 5555 / 6121 4444

F: (91–22) 2287 5771

E: emails@rsmindia.in

W: www.rsmindia.in

Offices: Mumbai, New Delhi–NCR, Chennai, Kolkata, Bengaluru, Surat, Hyderabad, Ahmedabad, Pune, Gandhidham and Jaipur.



facebook.com/RSMIndia



twitter.com/RSM_India



linkedin.com/company/rsm-india

RSM Astute Consulting Pvt. Ltd. (including its affiliates) is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network.

Each member of the RSM network is an independent accounting and consulting firm, each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction.

The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London, EC4N6JJ.

The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

In this publication, we have endeavoured to touch upon the key aspects of internal audit function keeping in mind the traditional success factors, the present trends and an eye on the Future of Internal Audit in the ever-changing business environment and digital arena. This publication should not be relied upon for taking actions or decisions without appropriate professional advice and it may be noted that nothing contained in this publication should be regarded as our opinion and facts of each case will need to be analysed based on specific facts. While all reasonable care has been taken in preparation of this publication, we accept no responsibility for any liability arising from any statements or errors contained in this publication.