Internal Audit: Risk and Tech Paradigm

Internal Audit (IA) provides independent assurance on the effectiveness of internal controls and risk management processes to enhance governance and achieve organisational objectives. IA is an independent management function, which involves a vital appraisal of the functioning of an entity with a view to suggest improvements and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management, internal control system, processes and procedures. Read on...

Aditya Maheshwari

The author is a member of the Institute. He can be reached at aditya.s.maheshwari@gmail.com and eboard@icai.in

If quantum of assurance could be reliably measured then it could be evidenced that IA function provides the maximum quantum of assurance given its significant value addition for management and statutory auditors. Successful IA encompasses management audit, operations audit, regulatory audit and systems audit in addition to its focus on audit of monetary transactions. It is a constructive feedback exercise for improving record to report process by reducing errors, oversights and frauds. The successful Internal Auditor is thus both a watch dog and a blood hound depending on the focus scenario and problem statement.

As per Section 138 of the Companies Act 2013 read with Rule 13 of the Companies (Accounts) Rules, 2014, the following class of companies shall be required to appoint an Internal Auditor or a firm of Internal Auditors, *viz.,*:-

(a) Every listed company;

(b) Every unlisted public company having–

(i) paid up share capital *of* INR 50 crore or more during the preceding FY; or

(ii) turnover (income) *of* INR 200 crore or more during the preceding FY; or

(iii) outstanding loans *or borrowings from banks or public financial institutions exceeding* INR 100 crore or more at any point of time during the preceding FY; or

(iv) outstanding deposits *of* INR 25 crore or more at any point of time during the preceding FY; and

(c) Every private company having–

(i) turnover of INR 200 crore or more during the preceding FY ; or

(ii) outstanding loans or borrowings from banks or public financial institutions exceeding INR 100 crore or more at any point of time during the preceding FY.

Basic Principles of IA

Basic Principle	Summary of Principle	Primary Quotient
Independence	Be free from any undue influences which force to deviate from the truth. This independence shall be both in actuality and appearance.	SQ
Integrity and Objectivity	Be truthful, unbiased and possess high integrity. Avoid all conflicts of interest and not seek or derive any undue personal benefit or advantage.	SQ
Due Professional Care	Exercise reasonable care expected of a professional to ensure successful achievement of planned objectives.	IQ
Confidentiality	Not to disclose information to a party outside the IA function except on a "need to know basis" or unless there is a legal or a professional responsibility to do so.	EQ
Skills and Competence	Have sound knowledge, strong interpersonal skills, practical experience and professional expertise required to conduct a quality audit.	IQ
Risk Based Audit	Identify the important audit areas through a risk assessment exercise and customise the audit activities such that the detailed audit procedures are prioritised and conducted over high risk areas, while less time is devoted to low risk areas through curtailed audit procedures.	IQ
Systems and Process Focus	Root cause analysis to be conducted on deviations to identify opportunities for improvement or automation and to strengthen the process and prevent a repetition of such errors.	IQ
Participation in Decision Making	Avoid passing any judgement or render an opinion on management decisions and avoid participation in operational decision making which may be subject of a subsequent audit.	EQ
Sensitive to Multiple Stakeholder Interests	Remain objective and present a balanced view where diverse interests may be conflicting in nature.	EQ
Quality and Continuous Improvement	Have a quality control process to ensure factual accuracy of the observations; to validate the accuracy of all findings; and continuously improve the quality of the IA process.	IQ

Standards on IA

The Standards on IA (SIA) are a set of minimum requirements or rules based on the basic principles enshrined above that apply to all the ICAI members while performing IA of any entity. The ICAI also recommends the adoption of the SIAs by non-ICAI members who are performing IAs so as to ensure a consistent approach and quality in the discharge of their professional duties. The current law in India permits IA to be performed either by an entity's own employee or by a professional who is part of an external agency. These SIAs apply to ICAI members in both situations, irrespective of whether the IA is conducted by them in the capacity of an employee or as a representative of an external agency.

The ICAI Council has decided that these Standards will be made mandatory in a phased manner. Accordingly the SIAs shall initially be mandatory for members performing IAs in all listed companies from the effective date of the SIA, and all other companies from one year thereafter. The mandatory status of a SIA implies that while carrying out an IA, it shall be the duty of the members of the ICAI to ensure that they comply with the SIAs read with the Preface, Framework Governing IAs and Basic Principles of IA. If a member is unable to comply with any of the SIAs requirements, or if there is a conflict between the SIA and other mandates, such as a regulatory requirement, the IA report should draw attention to the material departures therefrom along with appropriate explanation.

Below is the listing of prevalent SIA:

100 Series: Standards on Key Concepts • SIA 110, Nature of Assurance • SIA 120, Internal Controls	**200 Series: Standards on IA Management** • SIA 210, Managing the IA Function • SIA 220, Conducting Overall IA Planning • SIA 230, Objectives of IA • SIA 240, Using the Work of an Expert
300–400 Series: Standards on the Conduct of Audit Assignments • SIA 310, Planning the IA Assignment • SIA 320, IA Evidence • SIA 330, IA Documentation • SIA 350, Review and Supervision of Audit Assignments • SIA 360, Communication with Management • SIA 370, Reporting Results • SIA 390, Monitoring and Reporting of Prior Audit Issues	**Standards issued up to July 1, 2013** • SIA 5, Sampling • SIA 6, Analytical Procedures • SIA 7, Quality Assurance in IA • SIA 11, Consideration of Fraud in an IA • SIA 13, Enterprise Risk Management • SIA 14, IA in an Information Technology Environment • SIA 17, Consideration of Laws and Regulations in an IA • SIA 18, Related Parties

Risk Based Audit (RBA)

As mandated by the Basic Principles and SIA, the Internal auditor is required to identify the important audit areas through a risk assessment exercise and customise the audit activities such that the detailed audit procedures are prioritised and conducted over high risk areas and issues, while less time is devoted to low risk areas through curtailed audit procedures. This approach ensures that risks under consideration are more aligned to the overall strategic and company objectives rather than narrowly focused on process objectives.

An Internal Auditor should adopt a system and process focused methodology in conducting audit procedures. This methodology is more sustainable than the one adopted to test transactions and balances as it goes beyond "error detection" to include "error prevention". It requires a root cause analysis to be conducted on deviations to identify opportunities for systems improvement or basic principles automation, to strengthen the process and prevent a repetition of such errors.

Deployment of Information Technology (IT) by companies is now ubiquitious and should be understood for effective IAs. This helps the Internal auditor to move away from "people to process" and from "detection to prevention". IT spectrum needs to be increasingly overarched in identifying and for continuous monitoring of Standard Operating Processes (SOP), Key Risk Indicators (KRI) and Red Flags.

Risk is an event which can prevent, hinder, fail to further or otherwise obstruct the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise's ability to maximize stakeholder value and to achieve its business objectives. Risk can cause financial disadvantage or it can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the product of probability of occurrence of an event and the financial impact of such occurrence to an enterprise.

Risk may be broadly classified into Strategic, Operational, Financial and Knowledge:

Strategic Risks are associated with the long-term purpose, objectives and direction of the business.

Operational Risks are associated with the on-going, day-to-day operations of the enterprise.

Financial Risks are related specifically to the processes, techniques and instruments utilised to manage the finances of the enterprise, as well as Enterprise Risk Management those processes involved in sustaining effective financial relationships with customers and third parties.

Knowledge Risks are associated with the management and protection of knowledge and information within the enterprise.

Enterprise Risk Management (ERM)

ERM enables management to effectively deal with risk, associated uncertainty and enhancing the capacity to build value to the entity or enterprise and its stakeholders. Internal Auditor may review each of these activities and focus on the processes used by management to report and monitor the risks identified.

ERM is a structured, consistent and continuous process of measuring or assessing risk and developing strategies to manage risk within the risk appetite. It involves identification, assessment, prioritization, mitigation, planning, monitoring, assurance and implementation of risk and developing an appropriate risk response policy. Management is responsible for establishing and operating the risk management framework.

IA is a key part of the risk management lifecycle. The corporate risk function establishes the policies and procedures, and the assurance phase is accomplished by IA. The role of the Internal Auditor in relation to ERM is to provide assurance to management on the effectiveness of risk management. The scope of the Internal Auditor's work in assessing the effectiveness of the ERM would, normally, include assessing the:

- Risk maturity level;
- Adequacy of and compliance with the risk management policy and framework;
- Efficiency and effectiveness of the risk response; and
- Residual risk is to ensure that it is within the risk appetite.

The extent of Internal Auditor's role in ERM will depend on other resources available to the Board and on the risk maturity of the organisation. The nature of Internal Auditor's responsibilities should be adequately documented and approved by those charged with governance. The Internal Auditor has to review the structure, effectiveness and maturity of an enterprise risk management system. In doing so, he should consider whether the enterprise has developed a risk management policy setting out roles and responsibilities and framing a risk management activity calendar. The Internal Auditor should review the maturity of an ERM structure by considering whether the framework so developed, inter alia:

- Protects the enterprise against surprises;
- Stabilizes volatility;
- Operates within established risk appetite;
- Protects ability of the enterprise to attend to its core business; and
- Proactively manage risks.

The Internal Auditor will normally perform an annual risk assessment of the enterprise, to develop a plan of audit engagements for the subsequent period. This plan will be reviewed at various frequencies in practice. This typically involves review of the various risk assessments performed by the enterprise, consideration of prior audits, and interviews with senior management. The risk assessment process should be of a continuous nature so as to identify not only residual or existing risks, but also emerging risks. The risk assessment should be conducted formally at least annually, but more often in complex enterprises. To serve this objective, the Internal Auditor should design the audit work plan by aligning it with the objectives and risks of the enterprise and concentrate on those issues where assurance is sought by those charged with governance.

The risk review process to be carried out by the Internal Auditor provides the assurance that there are appropriate controls in place for the risk management activities and that the procedures are understood and followed. Effective enterprise risk management requires a monitoring structure to ensure that the risks are effectively identified and assessed and that the appropriate mitigation plans are in place.

The review process conducted by Internal Auditors will help to determine, inter alia:

- Adopted measures result in what was intended;
- Procedures adopted and information gathered for undertaking the assessment were appropriate; and
- Improved knowledge would help in reaching better decisions and identifying the lessons to improve future assessment and management of risks.

The Internal auditor should submit his report delineating the assurance rating (segregated into High, Medium or Low) as a result of the review.

Information Technology (IT) and Enterprise resource planning (ERP)

Contemporary technology could be harnessed for IA - Management by Objectives (MBO) and for being comprehensively compliant with the professional pronouncements and contractual covenants.

IT revolution has transformed the business landscape drastically by changing the manner of running and leading businesses. More lately, developments around

Artificial Intelligence (AI), Block Chain, Big Data, Internet of Things (IoT) and Cloud Computing have been moving the business paradigm to next plane and at an unprecedented pace. IA domain could leverage on these developments in a calibrated manner to reinforce its value addition to the overall business management and the global economy.

IT systems need to be deployed in such a manner to support IA delivery. IT could help the IA domain both actively and passively in facing and tiding over the challenges faced by the engagement executives and other stakeholders related to effective reporting, regulatory oversight, accountability clash between IA professionals and auditees, significance assigned to, managerial will and consequent budget allotted for the IA function alongwith overall social fabric for effective field work. SQL (Structured Query Language) and DBMS (Database Management Systems) supported functionalities could be deployed to enhance the review quality of the IA function by using various collaborative tools speeding-up the learning and the maturity level of the IA domain in the entity. Online surveys and voting led balanced scorecards could extensively be used for measuring the performance and appraisal of the IA function.

ERP is an integrated management of business processes in real time mediated by systems and technology. ERP systems incorporate best practices which in turn ease compliance with requirements such as Ind-AS, SEBI (Listing Obligations and Disclosure Requirements), ICOFR or Basel *et al*. ERP suitably accommodates RBA, ERM and myriad audit functionalities by keeping a chronological history of every transaction (time stamping); providing a comprehensive enterprise view; bringing legitimacy and drill-down of each bit of data; and providing increased opportunities for collaboration.

Advanced IT capabilities could help IA with:

- Focussing on areas of value to the organization iterating between a top-down approach and *vice versa*;
- Engagement of stakeholders through End User Computing (EUC) *viz.*, project trackers, PERT (Programme Evaluation and Review Technique)/ CPM (Critical Path Method) charts, RACI (Responsible, Accountable, Consulted, Informed) matrices, Heat Maps and Macros (Bot's);
- Making the IA function modular, scalable and dynamic;
- Built-in remediation and email-based notifications;
- Audit plan, programme and sampling;
- Real-time reports and exception reports;
- Configurable, role based and interactive dashboard;
- Issue life cycle management (CAPA – Corrective Action / Preventive Action), multi-year planning, risk assessment;
- Enhancement of organisation learning;
- BYoD (Bring Your Own Device) implementation and synchronised remote working;
- Engaging presentations;
- Paperless task and workflow management (audit trails, evidences, documentation, audit templates, checklists and document control);
- Alignment with COBIT and COSO frameworks;
- Collaborating with DMAIC model (Define, Measure, Analyze, Improve, Control) of Six Sigma;
- Specialized engagements (data analytics, fraud investigations, project monitoring, ERP implementation, revenue assurance and due diligence).

Takeaway

Lawrence Sawyer, the "Father of Modern IA" encouraged the modern Internal Auditor to act as a counsellor to management rather than as an adversary. Sawyer also insisted on providing recognition and positive reinforcement by capturing positive observations in audit reports. He underscored the benefits of providing more balanced reporting while simultaneously building better rapports and relationships catapulting the role of Internal Auditors from being bean-counters to become missionaries for a better governed corporate world.

Modern day technology subsumes a part of IQ (Intelligence Quotient) faction of the IA function liberating the IA professionals to focus more on the SQ (Spirituality Quotient) and EQ (Emotional Quotient) components. Thus tech-supported risk based IA delivery for MSME to MNC entities speeds-up 360^0 transition towards the Swayer's vision for the IA fraternity. ■

References:

- Preface to the Framework and Standards on IA; Framework Governing IAs; Basic Principles of IA; SIA (ICAI)
- Sawyer, Lawrence (2003) Sawyer's Internal Auditing 5th Edition