Internal Audit – SIAs, Codifying the Best Practices

CA. Rajkumar S Adukia
B.Com (Hons), FCA, ACS, ACWA, LLB, DIPR, DLL &LP, IFRS(UK), MBA
email id: rajkumarradukia@caaa.in
Mob: 09820061049/09323061049

To receive regular updates kindly send test email to : rajkumarfca-subscribe@yahoogroups.com & rajkumarfca+subscribe@googlegroups.com

What is an Internal Audit/Assurance Work?

- A management function
- Internal auditors to render impartial judgments
- It is a dynamic one
- It assists board in governance responsibility
- Auditor assures the effectiveness of internal audit
- It is a component of internal control

Origin of Internal Audit Function

- Internal Audit dates back to 5000 BC.
- Chaldae an Empire and the Babylonian Empire where the first to introduce Internal Control System
- Internal Audit began during the Second World War when organisations found it difficult to maintain operational efficiency and control.

Internal Audit/Assurance Cycle

- Pre engagement activity
- Understanding the work
- Assurance plan
- Substantive work
- Report

What is Statutory Audit?

Statutory Audit is an audit required under law. *Statutory audit* is performed by the external auditor. It is mandatory on the part of the organization to get its accounts audited. In most of the cases the audit report forms part of the annual report of the organizations.

List of Statutory Audit Services

1. Audit under Income Tax Act 1961
2. Audit of Co-operative Societies
3. Audit of Multi State Cooperative Societies
4. Audit of NBFC
5. Audit of Mutual Funds

List of Statutory Audit Services

6. Audit of Insurance Companies
7. Audit of Banks
    6. Accounting System in Banks
    7. Branch Audit
    8. Head Office Audit
    9. Long Form Audit – Branch Level
    10. Long Form Audit – HO Level
8. Audit of Companies

Definition of Internal Audit

"*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 system.*"- Preface to SIA

Scope of Internal Audit

- Evaluating the adequacy of internal controls
- Suggesting ways to reduce the costs and promote efficiency
- Assessing the compliance with the applicable laws and regulations
- Assist management in decision making
- Backbone of a sound corporate governance system

Need for Internal Audit

- Increased complexity of businesses
- Enhanced compliance requirements
- Focus on risk management and internal controls to manage them
- Unconventional business models
- Intensive use of information technology
- Stringent norms mandated by regulators to protect investors
- An increasingly competitive environment

IAASB

- International Auditing and Assurance Standard Board (IAASB) originally known as IAPC – International Auditing Practices Committee created in 1978
- The IAASB has published 32 International Standards on Auditing (ISAs) and approximately 20 International Auditing Practice Statements (IAPSs) and other pronouncements on topics such as quality control.

IAASB

- In the year 1979, The IAPC issued its first International Auditing Guideline, Objective and Scope of the Audit of Financial Statements
- In the year 1991, IAPC guidelines were recodified as International Standards on Auditing (ISAs)
- In the year 2002, IAPC was reconstituted as IAASB

Evolution of Auditing Standards in India

- Auditing Sub-Committee of Research Committee (ASRC) was constituted in the year 1955
- In 1963 ASRC issued the Statement on Auditing Practices
- In 1983 the Auditing Practices Committee (APC) was constituted which issued the first Auditing Standard in the year 1985.

Evolution of Auditing Standards in India

- In July 2002, APC was changed into Auditing & Assurance Standard Board (AASB)
- There are 43 Standards on Audit and Assurance work including those related to quality control, assurance engagement and related services issues by ICAI
- Auditing and Assurance Standards (AAS) have been changed to Standards on Auditing (SA) w.e.f 1.4 .2008.

Formation of Internal Audit Standards Board (IASB) - ICAI

- The Institute of Chartered Accountants of India constituted the “Committee for Internal Audit (CIA)” on 5th February 2004.
- At its 245th meeting held on November 29, 30 and December 1, 2005, the Council of the Institute of Chartered Accountants of India changed the nomenclature of the “Committee *for* Internal Audit” to “Committee on Internal Audit”.
- Further, at its 282nd meeting held on November 5–7, 2008, the Council has renamed the “Committee on Internal Audit” to “Internal Audit Standards Board (IASB)”.

Why do we need to Standards on Auditing?

- Adherence to standards on auditing enables an auditor to safe guard himself from professional negligence as stated under Clause 9 of Schedule II to the CA Act of 1949.
- There is a uniform and comprehensive coverage towards auditing.

Framework for Standards on Internal Audit

- The framework aims at promoting professionalism in Internal Audit Activity
- The framework applied to all persons performing internal audit activity , whether it is performed in house or by an external agency
- The framework consists of 4 components
  - Code of Conduct
  - The Competence Framework
  - The Body of Standards
  - The Technical Guidance

Code of Conduct

- Establishes the essential principles of conduct
- Prescribes Ethical Behavior
- Member of ICAI carrying our IA activity is covered by
  - The Chartered Accountant Act, 1949
  - Code of Ethics issued by ICAI
  - Other relevant pronouncements of ICAI

The Competence Framework

- The Competence Framework addresses the key characteristics that are required of persons performing internal audit.
- This includes aspects, such as, objectivity, technical competence, interpersonal skills, operational efficiency and due professional care.

The Body of Standards

- The Standards will specify basic principles and processes, such as defining the scope, planning, communicating, etc.
- Establish the basis for quality and performance evaluation of internal audit.

The Technical Guidance

- Technical Guidance can take 2 forms
  - Explanatory Material on the Standards
  - Application of Standards in Specific Industries or situations in the form of Technical Guides
- Helps in resolving professional issues arising in the course of performing IA activity

The first three components of the Framework for Standards on Internal Audit *viz.*,

the Code of Conduct,

the Competence Framework and

the Body of Standards

shall be **MANDATORY**.

List of SIA

Standards on Internal Audit

There are 17 Standards on Internal Audit (SIA) issued by ICAI

1. Standard on Internal Audit (SIA) 1, Planning an Internal Audit
2. Standard on Internal Audit (SIA) 2, Basic Principles Governing Internal Audit
3. Standard on Internal Audit (SIA) 3, Documentation
4. Standard on Internal Audit (SIA) 4, Reporting
5. Standard on Internal Audit (SIA) 5, Sampling
6. Standard on Internal Audit (SIA) 6, Analytical Procedures

List of SIA

7. Standard on Internal Audit (SIA) 7, Quality Assurance in Internal Audit
8. Standard on Internal Audit (SIA) 8, Terms of Internal Audit Engagement
9. Standard on Internal Audit (SIA) 9, Communication with Management
10. Standard on Internal Audit (SIA) 10, Internal Audit Evidence
11. Standard on Internal Audit (SIA) 11, Consideration of Fraud in an Internal Audit
12. Standard on Internal Audit (SIA) 12, Internal Control Evaluation

List of SIA

13. Standard on Internal Audit (SIA) 13, Enterprise Risk Management
14. Standard on Internal Audit (SIA) 14, Internal Audit in an Information Technology Environment
15. Standard on Internal Audit (SIA) 15, Knowledge of the Entity and its Environment
16. Standard on Internal Audit (SIA) 16, Using the Work of an Expert
17. Standard on Internal Audit (SIA) 17, Consideration of Laws and Regulations in an Internal Audit

Categorization of IA Standards

- The IA standards can be categorized into 5
  - Pre engagement activity – SIA 8,15
  - Understanding the work – SIA 1,9,17
  - Assurance plan – SIA 2,7,13
  - Substantive work – SIA 3,5,6,10,11,12,14,16
  - Report – SIA 4

PRE ENGAGEMENT ACTIVITY
SIA 8,15

SIA 8, Terms of Internal Audit Engagement

- The terms of the engagement should be agreed before commencement of engagement.
- The terms of engagement should be approved by
  - the Board of Directors1 or
  - a relevant Committee thereof such as the Audit Committee or such other person(s) as may be authorized by the Board in this regard.
- Key elements of Terms of Engagement
  - Scope
  - Responsibility

SIA 8, Terms of Internal Audit Engagement

- Authority
- Confidentiality
- Limitations
- Reporting
- Compensation
- Compliance with Standards

Withdrawal from Engagement

In case the internal auditor is unable to agree to any change in the terms of the engagement and/ or is not permitted to continue as per the original terms, he should withdraw from the engagement and should consider whether there is an obligation, contractual or otherwise, to report the circumstances necessitating the withdrawal to other parties.

SIA 15, Knowledge of the Entity and its Environment

- Provide guidance on what constitutes the knowledge of an entity's business
- The internal auditor should obtain knowledge of the economy, the entity's business and its operating environment, including its regulatory environment and the industry in which it operates, sufficient to enable him to review the key risks and entity-wide processes, systems, procedures and controls.

SIA 15, Knowledge of the Entity and its Environment

- Prior to accepting an engagement, the internal auditor should obtain a preliminary knowledge of the industry and of the nature of ownership, management, regulatory environment and operations of the entity subjected to internal audit
- Sources of Information on Entity's Business
- Using the Knowledge about Business

SIA 15, Knowledge of the Entity and its Environment

- The internal auditor should consider how this knowledge acquired, affects his review of the internal controls and systems taken as a whole and whether his overall entity-wide assessment of systems, procedures, controls and risk management principles are consistent with his knowledge of the entity's business.
- Documentation

UNDERSTANDING THE WORK
SIA 1,9,17

SIA 1, Planning an Internal Audit

- Provide guidance in respect of planning an internal audit.
- The internal audit plan should be consistent with the goals and objectives of the internal audit function as listed out in the internal audit charter as well as the goals and objectives of the organization.
- Plan should be continuously reviewed
- Certain factors affect the planning process

SIA 1, Planning an Internal Audit

- The Planning Process
  - Obtaining Knowledge of the Business
  - Establishing the Audit Universe
  - Establishing the Objectives of the Engagement
  - Establishing the Scope of Engagement
  - Deciding the Resource Allocation
  - Preparation of Audit Programme

SIA 9, Communication with Management

- Provides a framework for the internal auditor's communication with management
- Identifies some specific matters to be communicated with the management as described in the terms of the engagement.
- **Matters to be communicated**
  - *Internal Auditor's Responsibilities in Relation to the Terms of Engagement*
  - *Planned Scope and Timing of the Internal Audit*
  - *Significant Findings from the Internal Audit*

SIA 9, Communication with Management

- The communication process
  - Establishing communication process
  - Forms of Communication
  - Timing of Communication
  - Adequacy of communication process

- Documentation

SIA 17, Consideration of Laws and Regulations in an Internal Audit

- Deals with the internal auditor's responsibility to consider laws and regulations when performing an internal audit
- The standard applies to other engagements in which the IA is specifically engaged to test and report separately on compliance with specific laws or regulations
- Responsibility of Management for Compliance with Laws and Regulations - It is the primary responsibility of management.

SIA 17, Consideration of Laws and Regulations in an Internal Audit

- Objectives of Internal Auditor are
  - obtain sufficient appropriate audit evidence
  - perform specified audit procedures to help identify instances of non-compliance
  - respond appropriately to non-compliance or suspected noncompliance with laws and regulations

- SIA distinguishes the internal auditor's responsibilities in relation to compliance with two different categories of laws and regulations as follows:

SIA 17, Consideration of Laws and Regulations in an Internal Audit

- Those laws and regulations generally recognised to have a direct effect on the determi nation of material amounts and disclosures in the financial statements such as tax and laws regulating the reporting framework
- Other laws and regulations that do not have a direct effect on the determination of the amounts and disclosures in the financial statements.

SIA 17, Consideration of Laws and Regulations in an Internal Audit

- The internal auditor shall perform certain audit procedures to help identify instances of non-compliance with other laws and regulations that may have a significant impact on the entity's functioning
- Matters relevant to the internal auditor's evaluation
  - potential financial consequences of non-compliance
  - Need to inform the management
  - Testing the going concern of the organization
- Evaluating the implications of non compliance

ASSURANCE PLAN
SIA 2,7,13

SIA 2, Basic Principles Governing Internal Audit

- Establish standards and provide guidance on the general principles governing internal audit.
- The internal auditor should be straightforward, honest and sincere in his approach to his professional work.
- The internal auditor should maintain the confidentiality of the information acquired in the course of his work.
- The internal auditor should exercise due professional care, competence and diligence expected of him while carrying out the internal audit.
- The internal auditor should document matters, which are important in providing evidence that the audit was carried out in accordance with the Standards on Internal Audit

SIA 2, Basic Principles Governing Internal Audit

- The internal audit plan should be based on the knowledge of the business of the entity
- The internal auditor should, based on his professional judgment, obtain sufficient appropriate evidence
- The internal auditor should carefully review and assess the conclusions drawn from the audit evidence obtained, as the basis for his findings contained in his report and suggest remedial action.

SIA 7, Quality Assurance in Internal Audit

- This Standard on Internal Audit shall apply whenever an internal audit is carried out
- Establish standards and provide guidance regarding quality assurance in internal audit.
- The quality assurance framework established by the person entrusted with the responsibility for the quality in internal audit should, therefore, cover all the elements of the internal audit activity.

SIA 7, Quality Assurance in Internal Audit

- The frequency of the external quality review should be based on a consideration of the factors such as the maturity level of the internal audit activity in the entity, results of the earlier internal audit quality reviews, feedbacks as to the usefulness of the internal audit activity from the customers of the internal audit, costs *vis a vis* perceived benefits of the frequent external reviews.

SIA 13, Enterprise Risk Management

- Provide guidance on review of an entity's risk management system during an internal audit
- 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 may be broadly classified into Strategic, Operational, Financial and Knowledge

SIA 13, Enterprise Risk Management

- Enterprise Risk Management 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, mitigation, planning and implementation of risk and developing an appropriate risk response policy.
- Management is responsible for establishing and operating the risk management framework.

SIA 13, Enterprise Risk Management

- The Enterprise Risk Management process consists of Risk identification, prioritization and reporting, Risk mitigation, Risk monitoring and assurance.
- The role of the internal auditor in relation to Enterprise Risk Management is to provide assurance to management on the effectiveness of risk management
- The nature of internal auditor's responsibilities should be adequately documented and approved by those charged with governance.

SIA 13, Enterprise Risk Management

- The internal auditor should submit his report to the Board or its relevant Committee, delineating the following information:
  - Assurance rating (segregated into High, Medium or Low) as a result of the review;
  - Tests conducted;
  - Samples covered; and
  - Observations and recommendations.

SUBSTANTIVE WORK
SIA 3,5,6,10,11,12,14,16

SIA 3, Documentation

- Provide guidance on the documentation requirements in an internal audit.
- Documentation refers to the working papers prepared or obtained by the internal auditor and retained by him in connection with the performance of his internal audit.
- Internal audit documentation may be recorded on paper or on electronic or other media.

SIA 3, Documentation

- Internal audit documentation should record
  - the internal audit charter,
  - the internal audit plan,
  - the nature,
  - timing and extent of audit procedures performed, and
  - the conclusions drawn from the evidence obtained.
- The internal audit documentation should cover all the important aspects of an engagement *viz.*,
  - engagement acceptance,
  - engagement planning,
  - risk assessment and assessment of internal controls,
  - evidence obtained and examination/evaluation carried out,
  - review of the findings,
  - communication and reporting and follow up.

SIA 3, Documentation

- The internal audit file should be assembled within sixty days after the signing of the internal audit report.
- The internal auditor should formulate policies as to the custody and retention of the internal audit documentation within the framework of the overall policy of the entity in relation to the retention of documents.

SIA 5, Sampling

- Provide guidance on the use of audit sampling in internal audit engagements.
- "Audit sampling" means the application of audit procedures to less than 100% of the items within an account balance or class of transactions
- When designing an audit sample, the internal auditor should consider the specific audit objectives, the population from which the internal auditor wishes to sample, and the sample size.

SIA 5, Sampling

- When determining the sample size, the internal auditor should consider sampling risk, the tolerable error, and the expected error.
- The internal auditor should select sample items in such a way that the sample can be expected to be representative of the population.

SIA 6, Analytical Procedures

- The internal auditor should apply analytical procedures as the risk assessment procedures
  - at the planning and overall review stages of the internal audit.
  - to obtain an understanding of the business, the entity and its environment and in identifying areas of potential risk.
  - at or near the end of the internal audit when forming an overall conclusion as to whether the systems, processes and controls as a whole are robust, operating effectively and are consistent with the internal auditor's knowledge of the business.

SIA 6, Analytical Procedures

- When analytical procedures identify significant fluctuations or relationships that are inconsistent with other relevant information or that deviate from predicted amounts, the internal auditor should investigate and obtain adequate explanations and appropriate corroborative evidence.
- The internal auditor may recommend appropriate courses of action, depending on the circumstances.

SIA 10, Internal Audit Evidence

- Provide guidance in respect of applicability of this standard during an internal audit.
- The scope of an internal audit is much broader in comparison to that of statutory audit
- Internal audit evidence is used by the internal auditor to support the facts and opinion contained in his report.
- Sufficiency and appropriateness are interrelated and apply to evidence obtained
- The reliability of the internal audit evidence depends on its source – internal or external and on its type.

SIA 10, Internal Audit Evidence

- The internal auditor obtains evidence by performing one or more of the following procedures:
  - Inspection
  - Observation
  - Inquiry and confirmation
  - Computation
  - Analytical review

SIA 11, Consideration of Fraud in an Internal Audit

- The primary responsibility for prevention and detection of frauds rests with management and those charged with governance.
- A system of internal control comprise of following five elements:
  - the control environment
  - entity's risk assessment process;
  - information system and communication;
  - control activities; and
  - monitoring of controls

SIA 11, Consideration of Fraud in an Internal Audit

- The internal auditor should obtain an understanding of the policies and procedures adopted by the management to identify risks
- The internal auditor should evaluate the mechanism in place for supervision and assessment of the internal controls
- The internal auditor should document fraud risk factors identified as being present during the internal auditor's assessment process and document the internal auditor's response to any other factors.

SIA 12, Internal Control Evaluation

- Provide guidance on the procedures to be followed by the internal auditor in evaluating the system of internal control in an entity
- Internal controls may be either preventive or detective.
- Preventive controls attempt to deter or prevent undesirable acts from occurring.
- Detective controls attempt to detect undesirable acts.

SIA 12, Internal Control Evaluation

- The Internal auditor should examine the continued effectiveness of the internal control system through evaluation and make recommendations, if any, for improving that effectiveness.
- The internal auditor should use professional judgment to assess and evaluate the maturity of the entity's internal control.

SIA 12, Internal Control Evaluation

- Based on the results of the tests of control, the internal auditor should evaluate whether the internal controls are designed and operating as contemplated in the preliminary assessment of control risk.
- The internal auditor should identify internal control weaknesses that have not been corrected and make recommendations to correct those weaknesses.

SIA 12, Internal Control Evaluation

- The internal auditor in his report to the management, should provide:
  - A description of the significant deficiency or material weakness in internal control.
  - His opinion on the possible effect of such weakness on the entity's control environment.

SIA 14, Internal Audit in an Information Technology Environment

- The overall objective and scope of an internal audit does not change in an IT environment
- The internal auditor should consider the effect of an IT environment on the internal audit engagement
- The internal auditor should have sufficient knowledge of the information technology systems to plan, direct, supervise, control and review the work performed.

SIA 14, Internal Audit in an Information Technology Environment

- If specialized skills are needed, the internal auditor should seek the assistance of a technical expert possessing such skills, who may either be the internal auditor's staff or an outside professional.
- The internal auditor should obtain an understanding of
  - the systems,
  - processes,
  - control environment,
  - risk-response activities and
  - internal control systems

SIA 14, Internal Audit in an Information Technology Environment

- The internal auditor should review whether the information technology system in the entity considers the confidentiality, effectiveness, integrity, availability, compliance and validity of data and information processed.
- The internal auditor should review the robustness of the IT environment and consider any weakness or deficiency in the design and operation of any IT control within the entity
- The internal auditor should document the internal audit plan, nature, timing and extent of audit procedures performed and the conclusions drawn from the evidence obtained.

SIA 16, Using the Work of an Expert

- The internal auditor should obtain technical advice and assistance from competent experts if the internal audit team does not possess the necessary knowledge.
- When the internal auditor plans to use the expert's work, he should satisfy himself as to the expert's skills and competence
- The internal auditor should seek reasonable assurance that the expert's work constitutes appropriate evidence in support of the overall conclusions

SIA 16, Using the Work of an Expert

- The internal auditor should not, normally, refer to the work of an expert in the internal audit report.
- While referring to such work of the expert, the internal auditor should outline the assumptions, broad methodology and conclusions of the expert

REPORT
SIA 4

SIA 4, Reporting

- Establish standards on the form and content of the internal auditor's report issued as a result of an internal audit performed by an internal auditor
- The internal auditor's report should contain a clear written expression of
  - significant observations,
  - suggestions/ recommendations based on the policies,
  - processes,
  - risks,
  - controls and transaction processing taken as a whole and
  - managements' responses.

SIA 4, Reporting

- Elements of Internal Audit Reporting
  - (a) Title;
  - (b) Addressee;
  - (c) Report Distribution List;
  - (d) Period of coverage of the Report;
  - (e) Opening or introductory paragraph:

    (i) identification of the processes/functions and items of financial statements audited; and

    (ii) a statement of the responsibility of the entity's management and the responsibility of the internal auditor;

SIA 4, Reporting

(f) Objectives paragraph - statement of the objectives and scope of the internal audit engagement;

(g) Scope paragraph (describing the nature of an internal audit):

(h) Executive Summary, highlighting the key material issues, observations, control weaknesses and exceptions;

(i) Observations, findings and recommendations made by the internal auditor;

(j) Comments from the local management;

(k) Action Taken Report – Action taken/not taken pursuant to the observations made in the previous internal audit reports;

(l) Date of the report;

(m) Place of signature; and

(n) Internal auditor's signature with Membership Number.

SIA 4, Reporting

- The internal auditor should
  - exercise due professional care
  - report should have an appropriate title expressing the nature of the Report
  - report should be appropriately addressed as required by the circumstances of the engagement.
  - the report should be in line with the terms of the engagement,

SIA 4, Reporting

- The report should name the specific location, which is ordinarily the city where the internal audit report is signed.
- The report should be signed by the internal auditor in his personal name. The internal auditor should also mention the membership number assigned by the Institute of Chartered Accountants of India in the report so issued by him.

Codification of Best Practices

- The codification of standards mitigates the risk of noncompliance.
- It is a major restructuring of auditing and reporting standards designed to simplify user access to all authoritative Standards on Auditing by providing the authoritative literature in a topically organized structure.

Benefits of Codification

The codification

- reduces the time and effort required to perform auditing research.
- brings uniformity in approach
- enhances compliance by making the auditing literature more useable.
- provides real-time updates.
- assists with international convergence.
- serves as the authoritative reference source for XBRL.
- makes it clear that guidance not contained in the codification is not authoritative and flattens the GAAP hierarchy to only two levels.

ISAE 3000

- Initially released in June 2000, International Standard on Assurance Engagements (ISAE 100) was designed to provide a basic framework for large scale audits concerned with non-financial data process monitoring.
- These types of audits include environmental, social and sustainability reports; auditing of information systems, internal control, and corporate governance processes; and compliance audits for grant conditions, contracts and regulations.

ISAE 3000

- Three years later, to clarify the definition of "moderate assurance engagements," ISAE 3000 was established to further address ethical requirements; quality control; engagement acceptance; planning; expert materials; obtaining evidence; documentation; and preparing assurance reports.
- Guidelines like ISAE 3000 give auditors parameters for addressing and illustrating findings of compliance and sustainability reporting processes of their clients.

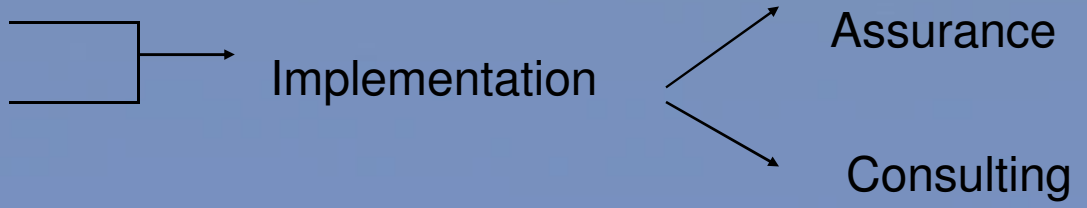
ISAE 3000

- No corresponding Standard on Auditing has been issued in India

The Institute of Internal Auditors (IIA)

IIA Hierarchy

- Mandatory Guidance
  - Definitions
  - Code of Ethics
  - Standards
    - Attributes
    - Performance



IIA Hierarchy

- Strongly Recommended Guidance
  - Position Papers
  - Practice Advisories
  - Practice Guides

IIA on Internal Audit

- The IIA guides the international profession of internal audit with not only Standards, but numerous additional resources to assist internal auditors worldwide implement best practices in our ever-changing and growing field.
- They are advisories, guides, papers, and tools

Audit Pronouncements of IIA

- Mandatory audit pronouncements of IIA are the “International Standards for Professional Practice of Internal Auditing (Standards)
- The standards are part of the “International Professional Practices Framework (IPPF)”

IPPF – International Professional Practices Framework

- State basic principles for practice of internal auditing
- Provide a framework for performing and promoting value-added internal auditing
- Establish the basis for evaluating internal audit performance
- Improve organizational processes and operations

International Standards for Professional Practice of Internal Auditing (Standards)

- The Standards consist of
  - Attribute Standards (1000-1322)
  - Performance Standards (2000-2600)
  - Implementation Standards (integrated with other standards)
- Attribute Standards are about the attributes of an organization and individuals providing internal auditing services
- Performance Standards describe the nature of internal auditing and quality criteria for evaluation of their performance.

International Standards

- Attribute Standards – 18
- Performance Standards - 31

COBIT

- **COBIT** is a framework created by ISACA for information technology (IT) management and IT Governance.
- It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
- It is an international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals.
- It is positioned at a high level and has been aligned and harmonized with other, more detailed, IT standards and good practices as COSO, ITIL, ISO 27000, CMMI, TOGAF and PMBOK

COBIT

- COBIT defines 34 generic processes to manage IT.
- Each process is defined together with process inputs and outputs, key process activities, process objectives, performance measures and an elementary maturity model.
- The framework supports governance of IT by defining and aligning business goals with IT goals and IT processes.

COBIT

- COBIT 5-Schedule to release in 2012,
- COBIT 5 will consolidate and integrate the COBIT 4.1, Val IT 2.0 and Risk IT frameworks and also draw significantly from the Business Model for Information Security (BMIS) and ITAF.

COBIT – Categories of Guidelines

I Plan and Organize – PO

- PO1 Define a Strategic IT Plan
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks
- PO10 Manage Projects

COBIT – Categories of Guidelines

II Acquire and Implement – AI

- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology Infrastructure
- AI4 Enable Operation and Use
- AI5 Procure IT Resources
- AI6 Manage Changes
- AI7 Install and Accredit Solutions and Changes

COBIT – Categories of Guidelines

III Deliver and Support – DS

- DS1 Define and Manage Service Levels
- DS2 Manage Third-party Services
- DS3 Manage Performance and Capacity
- DS4 Ensure Continuous Service
- DS5 Ensure Systems Security
- DS6 Identify and Allocate Costs
- DS7 Educate and Train Users
- DS8 Manage Service Desk and Incidents
- DS9 Manage the Configuration
- DS10 Manage Problems
- DS11 Manage Data
- DS12 Manage the Physical Environment
- DS13 Manage Operations

COBIT – Categories of Guidelines

IV Monitor and Evaluate – ME

- ME1 Monitor and Evaluate IT Performance
- ME2 Monitor and Evaluate Internal Control
- ME3 Ensure Compliance With External Requirements
- ME4 Provide IT Governance

COSO

- The Committee of Sponsoring Organizations' (COSO) mission is to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.
- COSO's vision is to be a recognized thought leader in the global marketplace on the development of guidance in the areas of risk and control which enable good organizational governance and reduction of fraud.

Enterprise Risk Management

What is ERM?

ENTERPRISE (E)	→	**GOALS (ORGANIZATION)**
RISK (R)	→	**EVENTS (OUTCOME)**
MANAGEMENT (M)	→	**ACTION (PRECAUTION)**

ERM

- Enterprise – “ Organization”, “Company”, “Institution”, “Business Set Up”
- Risk – “Danger”, “Loss”, “Obstacle”
- Management – “Handling”, “Getting what you want”, “Practical solution to the given circumstance”, “Avoiding a collapse”

RISK MANAGEMENT

Risk management is an attempt

- to identify,
- to measure,
- to monitor and
- to manage uncertainty.

Benefits of risk management

- Supports strategic And Business planning
- increased certainty and fewer surprises
- Better service delivery
- Quick grasp of new opportunities
- **Potential benefits**
- More efficient use of resources
- Reassures stakeholders
- Helps focus internal audit programme
- Promotes continual improvement

Definition of ERM

"Enterprise risk management is a

- ***process**,*
- ***effected** by an entity's board of directors,_management and other personnel,*
- ***applied** in strategy setting and across the enterprise,*
- ***designed***
- ***to identify** potential events that may affect the entity, and*
- ***manage risk** to be within its risk appetite,*
- *to provide reasonable **assurance***
- *regarding the achievement of **entity objectives**."*

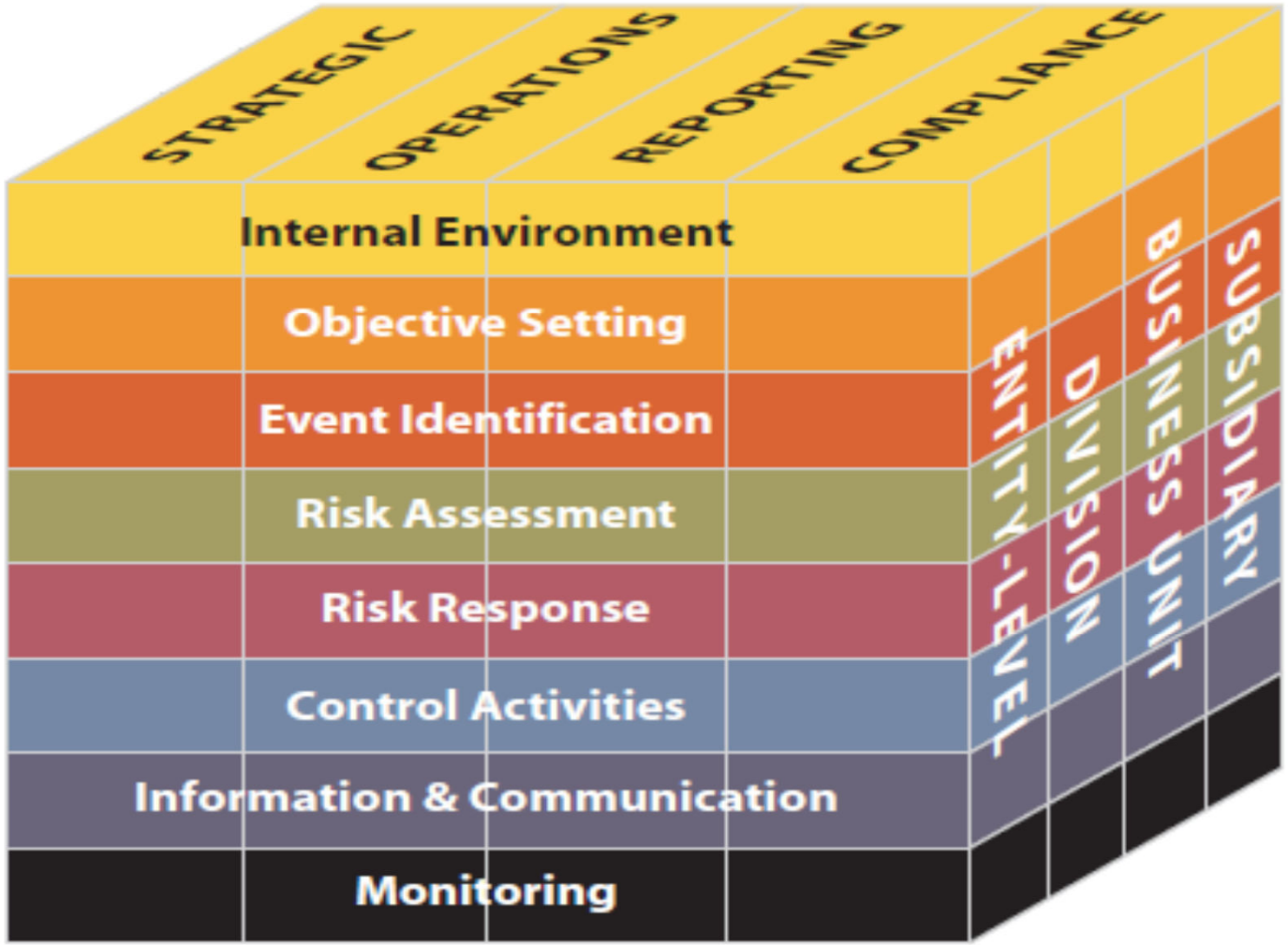
COSO (Committee of Sponsoring Organizations of the Treadway Commission) defines ERM

Enterprise – Entity's Objective

Entity's Objectives - 4 categories

- **Strategic** – high-level goals, aligned with and supporting its mission
- **Operations** – effective and efficient use of its resources
- **Reporting** – reliability of reportin
- **Compliance** – compliance with applicable laws and regulations

8 Components of ERM



8 Components of ERM

1. Internal Environment
2. Objective Setting
3. Event Identification
4. Risk Assessment
5. Risk Response
6. Control Activities
7. Information and Communication
8. Monitoring

Objectives of ERM

- Improve risk-based decision making
- More effective use of capital
- Comply with regulatory changes
- Improve shareholder value
- Anticipating problems before they become a threat
- Co-coordinating various risk management activities

ISO : 31000

- ISO 31000 was published in 2009 as an internationally agreed standard for the implementation of risk management principles
- ISO also produced Guide 73 ‘Risk management – Vocabulary – Guidelines for use in standards’.
- The definition set out in ISO Guide 73 is that risk is the “effect of uncertainty on objectives”.

ISO : 31000

- Guide 73 also states that an effect may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence.
- Risk management is a central part of the Strategic Management of any a organization
- Risk Architecture , Strategy and Protocols

ISO:31000

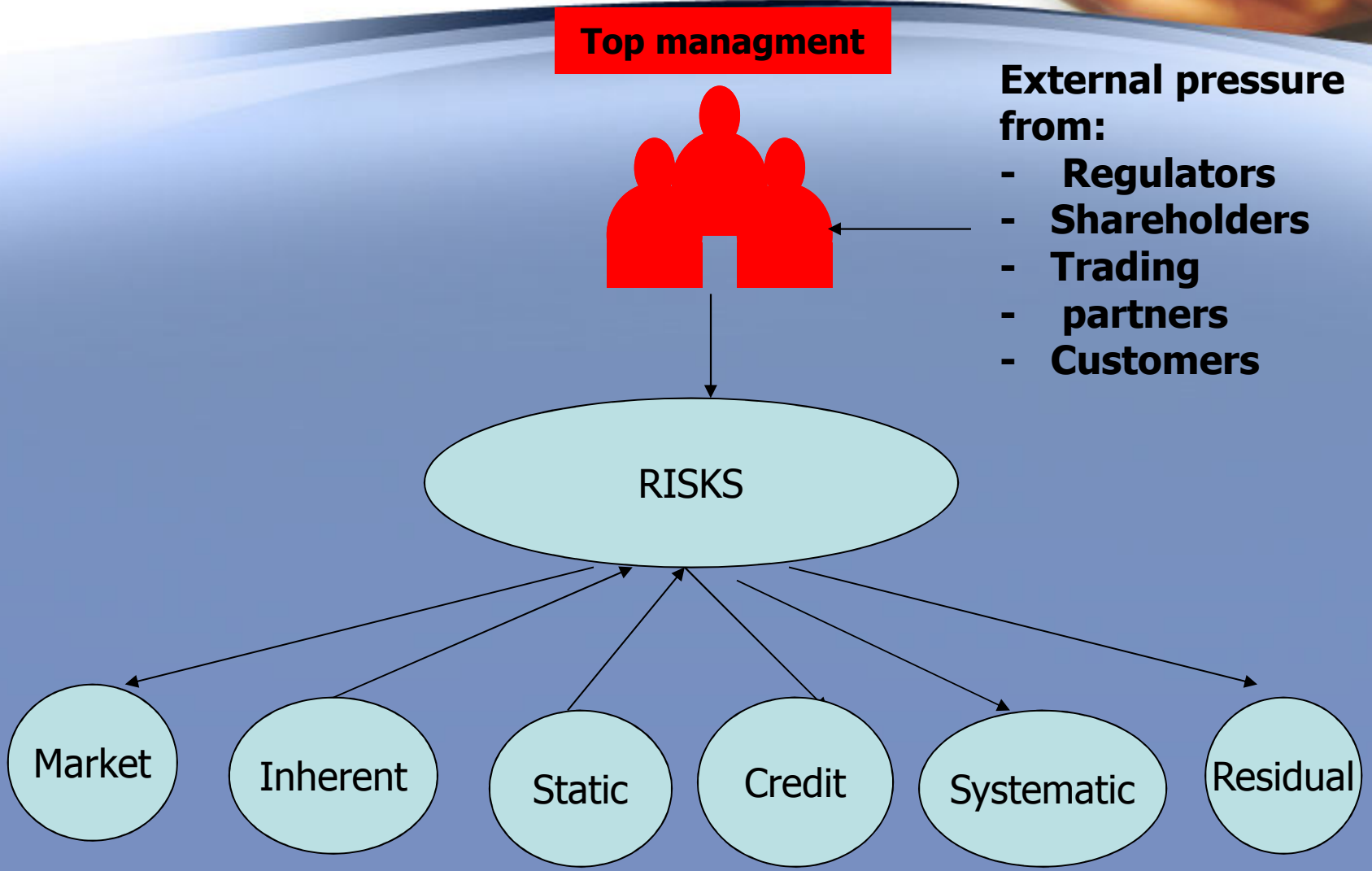
- ISO 31000 does not recommend a specific risk classification system and each organisation will need to develop the system most appropriate to the range of risks that it faces.
- ISO 31000 describes a framework for implementing risk management, rather than a framework for supporting the risk management process.
- Information on designing the framework that supports the risk management process is not set out in detail in ISO 31000.
- Framework for managing risk as per ISO 31000

ISO:31000

ISO 31000 recognizes the importance of feedback by way of two mechanisms.

- Monitoring and review of performance and
- Communication and consultation

Types of Risks



Risk Management and Business Continuity

Risk management is simply a practice of systematically selecting cost effective approaches for minimizing the effect of threat realization to the organization.

Business Continuity Planning (BCP) is a methodology used to create a plan for how an organization will resume partially or completely interrupted critical function (s) within a predetermined time after a disaster or disruption

Challenges

- Data availability & integrity
- Data warehousing/ mining
- Building up processes & systems
- Developing Human Resources
- Strengthening skills
- Model validation – requires greater collaboration with regulator
- Cost - investment in risk analytics and risk technology – getting management buy-in
- Stress testing, scenario analysis – building capabilities

Implementation Of ERM

The basic elements of an effective risk management program are:

1. **Senior management and board level commitment**
2. **Risk management policies and procedures established in writing for the most prominent risks, with specific objectives and targets**
3. **Clearly defined responsibilities for managing and controlling risk**
4. **Ongoing employee training is essential**
5. **Testing and monitoring of all programs and procedures**
6. **Regular reports including independent audits prepared for review by senior management and board directors**

Conclusion

- Banks and insurers will have different approaches to ERM, but should understand each other's methods and terminology
- Each type of institution has various strengths that can benefit other industries
- Regulation can generate arbitrage opportunities, internationally or across industries
- ERM is likely to be a growth area in insurance over the next decade

Role of Internal auditor

Support management by providing assurance on the

- ERM Process function
- .Effectiveness and efficiency of risk responses and control activities.
- Completeness and accuracy of ERM reporting

Why is ERM important?

- Identify obstacles to achieving business objectives
- Allow management to make/evaluate decisions on a well informed, risk adjusted basis
- Determine accountability/ownership of all key risks
- Enable definition of realistic tolerances and measures of risk to support reasonable budgeting for risk (expected loss) and allocation of capital (unexpected loss)

Why is ERM important?

- Increase risk and control awareness of all employees, at all levels
- Proactively identify potential difficulties
- Business continuity and disaster preparedness in a post-9/11 world
- Regulatory compliance
- Globalization in a continuously competitive environment

Risk management is a

Continuous Journey

About the Author

- *CA. Rajkumar S Adukia is an eminent business consultant, academician, writer, and speaker. He is the senior partner of Adukia & Associates.*
- *In addition to being a Chartered Accountant, Company Secretary, Cost Accountant, MBA, Dip IFR (UK), Mr. Adukia also holds a Degree in Law and Diploma in Labor Laws and IPR.*
- *Mr. Adukia, a rank holder from Bombay University completed the Chartered Accountancy examination with 1st Rank in Inter CA & 6th Rank in Final CA, and 3rd Rank in Final Cost Accountancy Course in 1983.*
- *He started his practice as a Chartered Accountant on 1st July 1983, in the three decades following which he left no stone unturned, be it academic expertise or professional development.*

.

About the Author

- *He has been coordinating with various Professional Institutions, Associations, Universities, University Grants Commission and other Educational Institutions.*
- *Authored more than 50 books on a vast range of topics including Internal Audit, Bank Audit, SEZ, CARO, PMLA, Anti-dumping, Income Tax Search, Survey and Seizure, IFRS, LLP, Labour Laws, Real estate, ERM, Inbound and Outbound Investments, Green Audit etc.*
- *The author can be reached at **rajkumarradukia@caaa.in** Mob – 09820061049 / 09323061049*
- *For more details log on to www.caaa.in*

Thank You