



Bombay Chartered Accountants' Society
The Knowledge Portal



Bombay Chartered Accountants' Society

Seminar on Internal Audit

November 21, 2009

Ashutosh Pednekar

Partner, M P Chitale & Co.

**Standards on Internal Audit
11 to 16**

SIA 11 to 16



- 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 Entity and its Environment
- SIA 16 → Using Work of an Expert

SIA 11 Consideration of Fraud in an Internal Audit



- Fraud is an intentional act by one or more individuals among management, those charged with governance, or third parties, involving the use of deception to obtain unjust or illegal advantage
 - Misstatement of an information (financial or otherwise) or
 - Misappropriation of the assets of the entity
- Primary responsibility for prevention and detection of frauds is of management & those charged with governance
 - IA should use his knowledge & skills to reasonably enable him to identify indicators of frauds
 - IA should help management fulfil its responsibilities relating to fraud prevention and detection

Elements of Internal Control Systems



■ Control Environment

- Obtain understanding of various aspects of control environment
- Evaluate same for its operating effectiveness

■ Entity's Risk Assessment Process

- Obtain understanding of policies and procedures adopted to identify risks
- Evaluate effectiveness of same
- Focus on policies & procedures to prevent frauds – those that identify & assess risks and frauds
 - Include possibility of fraudulent financial reporting and misappropriation of assets

Elements of Internal Control Systems



■ Information Systems & Communication

- Assess effectiveness of processes to identify, capture & communicate relevant information to enable timely and effective decisions

■ Control Activities

- Assess controls implemented to ensure risks identified are responded to as per management policy

■ Monitoring of Controls

- Evaluate mechanism for supervision and assessment of internal controls

Documentation & Communication



- Document fraud risk factors identified
- If necessary, based on above, additional procedures are to be done, then the same needs to be documented
- Communicate immediately any actual or suspected fraud

SIA 11 to 16



- 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 Entity and its Environment
- SIA 16 → Using Work of an Expert

SIA 12 Internal Control Evaluation



**Accuracy & completeness of
Accounting Records**

**Efficiency & effectiveness
in Operations**

**Reliability of
financial reporting**

**INTERNAL
CONTROL
SYSTEM
OBJECTIVES**

**Prevention &
Detection of Fraud &
Error**

**Compliance with
applicable laws
and regulations**

Safeguarding of Assets

Internal Control Components & IA



- IA is a separate component of internal control with the objective of determining whether they are well designed and properly operated

**Control (or Operating)
environment.**

Risk Assessment

**Control Objective
Settings**

Event Identification

Control Activities

**Information &
Communication**

Monitoring

Risk Response

Factors of Control Environment



- Entity's organisational structure
 - Segregation of duties & supervisory functions
- Function of Board of Directors & its Committees / Governance Body
- Management's philosophy & operating style
- Management's control system including
 - IA function
- Integrity & ethical values
- Commitment to competence
- HR policies & practices

Inherent Limitation of Internal Controls



- Management's consideration of **cost of control** being less than expected benefit
- Potential for **human error** including mistakes of judgement & misunderstanding of instructions
- **Collusion** – internally as well as externally
- **Abuse of power** – especially by those who exercise internal control
- **Manipulations by management** w.r.t transactions, estimates or judgements required to prepare financial statements

Role of IA



- IA to focus towards improving internal control structure & promoting better corporate governance
 - Obtain an understanding of significant processes & control systems
 - Use this to develop the audit plan
 - Use professional judgement to assess & evaluate maturity of internal controls
 - Assess management's attitudes, awareness and actions regarding internal controls
- Understand & document the design and operations of internal controls to evaluate its effectiveness
 - Narratives / Flowcharts / Questionnaires

Test of Controls



■ Evidence of effectiveness of

- Design of internal control systems
- Operation of internal control systems throughout the period
- Cost of control < Benefit of control

■ Methods include:-

- Inspection of documents
- Observation of internal controls
- Re-performance of controls
- Testing computerised controls

Communication by IA



- Significant control deficiencies to be communicated to management or those charged with governance
 - Possible effect of deficiency also to be communicated
 - Recommendations for control improvements to be given
- Includes earlier identified deficiencies that are not yet remediated
- If there is a weakness in design or operation of internal control then IA needs to communicate to the appropriate level of management as soon as practicable

SIA 11 to 16



- 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 Entity and its Environment
- SIA 16 → Using Work of an Expert

SIA 13 Enterprise Risk Management



■ Purpose of SIA

- To establish standards & give guidance on review of an entity's risk management systems as part of IA or a separate review process

■ ERM enables management to deal with

- Risk
- Associated uncertainty
- Enhance capacity to build value

■ IA may review each of these activities and focus on processes used by management to report & monitor risks identified

Risk



- **Risk** → an event that can prevent, hinder, fail to further the enterprise in achieving its objectives
- **Business risk** → the threat that an event or action will adversely affect an enterprise's ability to maximize stakeholder value and to achieve its business objectives
- **Consequences of Risk transpiring:-**
 - Financial disadvantage, for example, additional costs or loss of funds or assets.
 - Damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities.

Typ

Strategic Risks are associated with the primary 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, utilized to manage the finances of the enterprise and affecting financial relationships with customers and third parties.

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

ERM Process



- 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.
- 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.

ERM & IA



- IA to provide assurance to management in relation to effectiveness of ERM
- IA's responsibilities to this effect is to be documented and approved by those charged with governance
- IA **should not** manage risks on behalf of management or take risk management decisions
- IA **should not** assume accountability of risk management decisions taken by management
- For all this IA has to be truly & completely independent

ERM & IA...



- IA should review the maturity of ERM structure by considering whether the framework:-
 - Protects enterprises against surprises
 - Stabilizes overall performance with volatile earnings
 - Operates within established risk appetite
 - Protects ability of the enterprise to attend its core business
 - Creates a system to proactively manage risks
- Review whether ERM coordinators report to following as required:-
 - Enterprise Business & Unit Heads / RMC / Audit Committee

IA Plan based on Risk Assessment



- Internal audit plan should be approved by the audit committee
 - Be based on risk assessment as well as on issues highlighted by the audit committee and senior management.
- Risk assessment process should be of a continuous nature so as to identify not only residual or existing risks, but also emerging risks.
- 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.

Review Report



- IA to submit 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;
 - Observations and recommendations.

SIA 11 to 16



- 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 Entity and its Environment
- SIA 16 → Using Work of an Expert

SIA 14 IA in an IT Environment



- Fundamental Rule → **IA objective & scope does not change in an IT Environment**
- But IA has to consider the effect of the IT environment
 - To the extent to which it is used by the entity &
 - The related internal control w.r.t usage of IT
- For this skill & competence is required of the IA
 - Sufficient knowledge of IT systems to plan, direct, supervise, control & review the work performed
 - Whether any specialised IT skills needed to conduct audit of specialised systems
 - Specialized skills maybe in-house or obtained from an expert

Planning the Audit



- Obtain understanding of the significance & complexity of the IT activities:-
 - IT Infrastructure
 - Voluminous transactions or multifarious transactions transcending various applications
 - Lack of transaction trails
 - Uniform processing of transactions
 - Lack of segregation functions
 - Potential for errors & irregularities
 - Initiation or execution of transactions
 - Dependence of other controls over computer processing
 - Potential for increased management supervision
 - Potential for use of CAAT

Planning the Audit vis-à-vis Risk Assessment



- IA should evaluate the application of the CIA principle
 - Data is authorised, correct and complete
 - Timely detection & correction of errors
 - Recovery from interruption
 - Accuracy and completeness of output
 - Physical & environmental controls
 - Logical controls
 - Protecting the application systems and preventing unauthorised changes

Audit procedures



■ Review of

- System Audit reports

- Exceptional events identification & mitigation

 - System breaches / unauthorised logins / password compromises etc

 - Network failures / virus attacks and threats to perimeter security

- General physical, logical & environmental controls

- Application controls

- BCP / DRP

■ This is to be done for all outsourced activities also and with more diligence

SIA 11 to 16



- 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 Entity and its Environment
- SIA 16 → Using Work of an Expert

SIA 15 Knowledge of Entity & its Environment



- Purpose → to establish standards & guidance on
 - What is knowledge of business
 - Importance to various phases of IA
 - Techniques to be adopted
 - Prior to IA engagement & subsequently thereafter
 - Documentation of this knowledge

Entity's Operations & its Environment



- Prior to acceptance of IA engagement
 - Preliminary knowledge of industry
 - Nature of ownership
 - Nature of management
 - Regulatory requirements

- On acceptance of engagement → more detailed information should be obtained
 - Continuous assessment, enhancement updation, refinement & validation is required

Sources on Information



- Previous engagement experience with entity & industry
- Business plan
- Organisational structure & hierarchy
- Discussions with
 - Key management persons
 - Statutory auditors
 - Other auditors, legal and other advisors
 - Knowledgeable experts outside the entity
- Industry publications / trade journals
- Legislations & regulations
- Visit to plants, premises, depots etc
- Internal documentation – minutes etc
- Annual reports and website
- SOPs & Manuals

Using the knowledge



- Use it in evaluation of risk assessment and controls
- Ensure entire IA engagement team has adequate knowledge
- Plan the IA accordingly
- Determine appropriate materiality levels
- Document all above in engagement working papers

SIA 11 to 16



- 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 Entity and its Environment
- SIA 16 → Using Work of an Expert

SIA 16 Using Work of an Expert



- Purpose → establish standards and provide guidance when IA should use an expert
- If IA does not possess necessary knowledge, skills, expertise then he approaches competent experts and obtain technical advice
- Expert has to be independent
- IA to satisfy himself about Expert's competence, objectivity & independence
 - More so, if expert is chosen by senior management or those charged with governance

Work of the Expert



■ When to use Expert:-

- Materiality of item being examined
- Nature & complexity of item including the risk of error therein

■ Skill & competence of Expert:-

- Expert's professional qualifications / membership in appropriate professional body
- Reputation of expert
- Knowledge and specific experience of expert in the entity's industry

Work of the Expert...



■ Objectivity of Expert:-

- No personal, financial or organisational interests of expert with the entity that will prevent him from giving impartial judgement / opinion
- If answer is negative, then determine whether another expert is required or whether more extensive audit procedures are required to be deployed

Work of the Expert...



- Evaluating the Work of Expert:-
 - Terms of reference given to him
 - Independence & objectivity observed
 - Source data used
 - Assumptions made and methods used and their consistency over prior periods
 - Making inquiries with the Expert
 - Comparing Expert's opinion with own IA findings
- If work of expert does not support related representations in overall systems, procedures and controls, then IA should attempt to resolve inconsistency by discussing with the auditee and the expert

Reference in IA Report



- IA should not, normally, refer to work of an expert in the IA report
- Reference is given when IA feels that the reader will understand the report better
- IA should outline the assumptions, broad methodology and conclusions of the expert
- If IA feels so, identity of expert can be given
 - Prior consent of expert is required

Thank you

ashu01@mpchitale.com

