

STANDARD ON INTERNAL AUDIT (SIA) 17

CONSIDERATION OF LAWS AND REGULATIONS IN AN INTERNAL AUDIT

Contents

Paragraph(s)

Scope.....	1
Definition	2
Effect of Laws and Regulations	3-4
Responsibility of Management for Compliance with Laws and Regulations.....	5-6
Objectives	7
Responsibility of the Internal Auditor	8-21
The Internal Auditor's Consideration of Compliance with Laws and Regulations.....	22-31
Internal Audit Procedures When Non-Compliance is Identified or Suspected	32-40
Reporting of Identified or Suspected Non-Compliance	41-45
Documentation	46-47
Effective Date	48

The following is the text of the Standard on Internal Audit (SIA) 17, Consideration of Laws and Regulations in an Internal Audit, issued by the Institute of Chartered Accountants of India. The Standard should be read in the conjunction with the "Preface to the Standards on Internal Audit", issued by the Institute.

In terms of the decision taken by the Council of the Institute at its 260th meeting held in June 2006, the following Standard on Internal Audit shall be recommendatory in nature in the initial period. The Standard shall become mandatory from such date as may be notified by the Council in this regard.

Standard on Internal Audit (SIA) 17

Scope

1. This Standard on Internal Audit (SIA) deals with the internal auditor's responsibility to consider laws and regulations when performing an internal audit. This SIA also applies to other engagements in which the internal auditor is specifically engaged to test and report separately on compliance with specific laws or regulations.

Definition

2. For the purposes of this SIA, the following term has the meaning attributed below:

Non-compliance – Acts of omission or commission by the entity, either intentional or unintentional, which are contrary to the prevailing laws or regulations. Such acts include transactions entered into by, or in the name of, the entity, or on its behalf, by those charged with governance, management or employees. Non-compliance does not include personal misconduct (unrelated to the business activities of the entity) by those charged with governance, management or employees of the entity.

Effect of Laws and Regulations

3. The effect on the functioning of an entity of laws and regulations varies considerably. Those laws and regulations to which an entity is subject to constitute the legal and regulatory framework. The provisions of some laws or regulations have a direct effect on the financial statements in that they determine the reported amounts and disclosures in an entity's financial statements. Other laws or regulations are to be complied with by management or set the provisions under which the entity is allowed to conduct its business but do not have a direct effect on an entity's financial statements. Some entities operate in heavily regulated sectors (such as banking, non-banking finance, insurance, telecom, etc.). Others are subject only to the many laws and regulations that relate generally to the operating aspects of the business (such as those related to environment, occupational safety and health).

4. Non-compliance with laws and regulations may result in fines, litigation or other consequences for the entity that may have a material effect on not only the reporting framework of the financial statements but also on the functioning of

Consideration of Laws and Regulations in an Internal Audit

the entity and which in extreme cases may impair their ability to continue as a going concern itself.

Responsibility of Management for Compliance with Laws and Regulations

5. It is the primary responsibility of management, with the oversight of those charged with governance, to ensure that the entity's operations are conducted in accordance with the provisions of laws and regulations, including compliance with the provisions of laws and regulations that determine the reported amounts and disclosures in an entity's financial statements.

6. The following are examples of the types of policies and procedures an entity may implement to assist in the prevention and detection of non-compliance with laws and regulations:

- Monitoring legal requirements and ensuring that operating procedures are designed to meet these requirements.
- Instituting and operating appropriate systems of internal control.
- Developing, publicising and following a code of conduct. Ensuring employees are properly trained and understand the code of conduct. Monitoring compliance with the code of conduct and acting appropriately to discipline employees who fail to comply with it.
- Targeting information for compliance to those employees or departments who are in the best position to verify possibilities of non-compliance.
- Engaging legal advisors to assist in monitoring legal requirements.
- Maintaining a register of significant laws and regulations with which the entity has to comply within its particular industry and a record of complaints.

These policies and procedures may be supplemented by assigning appropriate responsibilities to the following:

- A compliance function.
- An audit committee.

Standard on Internal Audit (SIA) 17

Objectives

7. The objectives of the internal auditor are:
- (a) To obtain sufficient appropriate audit evidence regarding compliance with the provisions of those laws and regulations generally recognised to have a direct effect on the determination of material amounts and disclosures in the financial statements;
 - (b) To perform specified audit procedures to help identify instances of non-compliance with other laws and regulations that may have a significant impact on the functioning of the entity; and
 - (c) To respond appropriately to non-compliance or suspected non-compliance with laws and regulations identified during the internal audit.

Responsibility of the Internal Auditor

8. Paragraph 3.1 of the "Preface to the Standards on Internal Audit", issued by the Council of the Institute of Chartered Accountants of India in 2007, describes internal audit as follows:

"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."

9. Compliance with laws and regulations is an inherent part of the functioning of an entity. Since the role of an internal auditor is to carry out a continuous and critical appraisal of the functioning of an entity and suggest improvements thereto, the identification of non-compliance with laws and regulations is also an inherent part of his responsibilities. It will be pertinent to add here that the scope of an internal audit as described in paragraph 9 of the Standard on Internal Audit (SIA) 1, "Planning an Internal Audit", is also affected by the statutory or regulatory framework in which the entity operates.

10. Unlike the statutory audit function, in which the auditor is responsible for identification of non-compliance with the laws and regulations with a view to

Consideration of Laws and Regulations in an Internal Audit

obtain reasonable assurance that the financial statements, taken as a whole, are free from material misstatements, whether caused by fraud or error, the responsibilities of an internal auditor are much wider. As discussed in Para 3 (v) of the Standard on Internal Audit (SIA) 1, "Planning an Internal Audit", internal audit helps, inter alia, amongst other things, in ensuring compliance with the applicable statutory and regulatory requirements.

11. The scope of internal audit is determined by the terms of engagement of the internal audit activity whether carried out in house or by an external agency. Hence, in the case of an internal audit, the terms of engagement are variable and have an impact on the responsibility of the management vis a vis the internal auditor. The terms of engagement amongst other things, generally, require the internal auditor to examine the status of compliance with various statutes governing the entity. Even in the absence of an explicit mention in the terms of the engagement, the internal auditor has to verify compliance with laws and regulations within the overall objectives of an internal audit, as discussed in paragraph 2 of the Standard on Internal Audit (SIA) 1, "Planning an Internal Audit" which are as follows:

- to suggest improvements to the functioning of the entity; and
- to strengthen the overall governance mechanism of the entity, including its strategic risk management as well as internal control system.

12. Paragraph 8 of the Standard on Internal Audit (SIA) 12, "Internal Control Evaluation", describes that the internal audit function adds value to an organisation's internal control system by bringing a systematic, disciplined approach to the evaluation of risks and by making recommendations to strengthen the effectiveness of risk management efforts. Further, as discussed in paragraph 10 of the Standard on Internal Audit (SIA) 12, one of the broad areas of review by the internal auditor in evaluating the internal control system, inter alia, includes accounting and financial reporting policies and compliance with applicable legal and regulatory standards.

13. At the same time, as discussed in paragraphs 8 and 9 of the Standard on Internal Audit (SIA) 12, it may be noted that though the internal auditor's evaluation of internal control involves assessing non-compliance with laws and regulations, the internal auditor is not vested with the management's primary responsibility for designing, implementing, maintaining and documenting internal control.

Standard on Internal Audit (SIA) 17

14. Paragraph 9 of the Standard on Internal Audit (SIA) 13, "Enterprise Risk Management", describes that "the internal auditor should not manage any of the risks on behalf of the management or take risk management decisions. The internal auditor should not assume any accountability for risk management decisions taken by the management. Internal auditor has a role only in advising on risk management and assisting in the effective mitigation of risk."

15. The internal auditor is expected to exercise due professional care while carrying out the internal audit in detecting non-compliance with laws and regulations. As discussed in paragraph 6 of the Standard on Internal Audit (SIA) 2, "Basic Principles Governing Internal Audit", due professional care, however, neither implies nor guarantees infallibility, nor does it require the internal auditor to travel beyond the scope of his engagement.

16. The requirements in this SIA are designed to assist the internal auditor in identifying the significant impact of non-compliance with laws and regulations on the functioning of the entity. However, in view of the inherent limitations on the role of the internal auditor as discussed above, the internal auditor is not responsible for preventing non-compliance and cannot be expected to detect non-compliance with all laws and regulations.

17. In conducting an internal audit of an entity, the internal auditor takes into account the applicable legal and regulatory framework. Owing to the inherent limitations of an internal audit, there is an unavoidable risk that some non-compliances with laws and regulations and consequential material misstatements in the financial statements may not be detected, even though the internal audit is properly planned and performed in accordance with the SIAs. In the context of laws and regulations, the potential effects of inherent limitations on the internal auditor's ability to detect non-compliance are greater for such reasons as the following:

- There are many laws and regulations, relating principally to the operating aspects of an entity that typically do not affect the financial statements and are not captured by the entity's information systems relevant to financial reporting.
- Non-compliance may involve conduct designed to conceal it, such as collusion, forgery, deliberate failure to record transactions, management override of controls or intentional misrepresentations being made to the

Consideration of Laws and Regulations in an Internal Audit

internal auditor.

- Whether an act constitutes non-compliance is ultimately a matter for legal determination by a court of law.

Ordinarily, the further removed non-compliance is from the events and transactions captured or reflected in the entity's information systems relevant to financial reporting, the less likely the internal auditor is to become aware of it or to recognise the non-compliance.

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

- (a) The provisions of those laws and regulations generally recognised to have a direct effect on the determination of material amounts and disclosures in the financial statements such as tax and laws regulating the reporting framework; and
- (b) Other laws and regulations that do not have a direct effect on the determination of the amounts and disclosures in the financial statements, but compliance with which may be fundamental to the operating aspects of the business, to an entity's ability to continue its business, or to avoid material penalties (for example, compliance with the terms of an operating license, compliance with regulatory solvency requirements, or compliance with environmental regulations). Non-compliance with other laws and regulations may result in fines, litigation or other consequences for the entity, the costs of which may need to be provided for in the financial statements, or may even have a significant impact on the operations of the entity, but are not considered to have a direct effect on the financial statements, as described in paragraph 18(a). Non-compliance with laws and regulations that have a significant impact on the operations of the entity may cause the entity to cease operations, or call into question the entity's continuance as a going concern. For example, non-compliance with the requirements of the entity's license or other entitlement to perform its operations could have such an impact (for example, for a bank, non-compliance with capital or investment requirements). To illustrate further, a Non Banking Financial Company might have to cease to carry on the business of a non-banking financial institution if it fails to obtain a certificate of registration issued under Chapter III B of the Reserve Bank of India Act, 1934 and if its Net Owned Funds are less than the amount specified by the

Standard on Internal Audit (SIA) 17

RBI in this regard. There are also many laws and regulations relating principally to the operating aspects of the entity that typically do not affect the financial statements and are not captured by the entity's information systems relevant to financial reporting. An example here could be an airline failing to meet the safety norms prescribed by the government leading to an uncertainty over continuance of its license to operate. Non-compliance with such laws and regulations may, therefore, have a significant impact on the functioning of an entity.

19. In this SIA, differing requirements are specified for each of the above categories of laws and regulations.

- For the category referred to in paragraph 18(a), the internal auditor's responsibility is to obtain sufficient appropriate audit evidence, in accordance with the Standard on Internal Audit (SIA) 10, "Internal Audit Evidence", about compliance with the provisions of those laws and regulations.
- For the category referred to in paragraph 18(b), the internal auditor's responsibility is limited to undertaking specified audit procedures to help identify non-compliance with those laws and regulations that may have a significant impact on the functioning of the entity.

20. Non-compliance by the entity with laws and regulations may result in a material misstatement of the financial statements and in some cases, may impact significantly the functioning of the entity itself. Whether an act constitutes non-compliance with laws and regulations is a matter for legal determination, which is ordinarily beyond the internal auditor's professional competence to determine. Paragraph 2 of Standard on Internal Audit (SIA) 16, "Using the Work of an Expert" states as follows:

"The internal auditor should obtain technical advice and assistance from competent experts if the internal audit team does not possess the necessary knowledge, skills, expertise or experience needed to perform all or part of the internal audit engagement."

Nevertheless, the internal auditor's training, experience and understanding of the entity and its industry or sector may provide a basis to recognise that some acts, coming to the internal auditor's attention, may constitute non-compliance with

Consideration of Laws and Regulations in an Internal Audit

laws and regulations.

21. The internal auditor may have a specific responsibility, one that may arise out of the terms of engagement or a law or a regulation or a standard applicable to the internal auditor, to communicate directly, the above mentioned issues to an appropriate authority within the entity or a regulator. In these circumstances, Standards on Internal Audit, SIA 4, “Reporting” and SIA 8, “Terms of Internal Audit Engagement”, deal with how these audit responsibilities should be addressed in the internal auditor’s report. Furthermore, where there are specific statutory reporting requirements, it may be necessary for the internal audit plan to include appropriate tests for compliance with those provisions of the laws and regulations.

The Internal Auditor’s Consideration of Compliance with Laws and Regulations

Obtaining an Understanding of the Legal and Regulatory Framework

22. As part of obtaining an understanding of the entity and its environment in accordance with Standard on Internal Audit (SIA) 15, “Knowledge of the Entity and its Environment”, the internal auditor shall obtain a general understanding of:

- (a) The legal, regulatory and the financial reporting framework applicable to the entity and the industry or sector in which the entity operates; and
- (b) How the entity is complying with that framework.

To obtain a general understanding of such a legal and regulatory framework, and how the entity complies with that framework, the internal auditor may, for example:

- Use the internal auditor’s existing understanding of the entity’s industry, regulatory and other external factors;
- Update the understanding of those laws and regulations that directly determine the reported amounts and disclosures in the financial statements;
- Inquire of management as to other laws or regulations that may be expected to have a significant effect on the operations of the entity;

Standard on Internal Audit (SIA) 17

- Inquire of management concerning the entity's policies and procedures regarding compliance with laws and regulations as well as ethical issues within the entity; and
- Inquire of management regarding the policies or procedures adopted for identifying, evaluating and accounting for litigation claims.

Laws and Regulations Generally Recognised to have a Direct Effect on the Determination of Material Amounts and Disclosures in the Financial Statements

23. Certain laws and regulations are well-established, known to the entity and within the entity's industry or sector, and relevant to the entity's financial statements (as described in paragraph 18(a)). They could include those that relate to, for example:

- The form and content of financial statements;
- Industry-specific financial reporting issues;
- Accounting for transactions under government contracts; or
- The accrual or recognition of expenses for income tax or retirement benefits.

24. Some matters may be relevant to specific assertions (for example, the completeness of income tax provisions), while others may be relevant to the financial statements as a whole (for example, the required statements constituting a complete set of financial statements).

25. The internal auditor shall obtain sufficient appropriate audit evidence regarding compliance with the provisions of those laws and regulations generally recognised to have a direct effect on the determination of material amounts and disclosures in the financial statements.

Procedures to Identify Instances of Non-Compliance – Other Laws and Regulations

26. The internal auditor shall perform the following 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:

Consideration of Laws and Regulations in an Internal Audit

- (a) Inquiring of management and, where appropriate, those charged with governance, as to whether the entity is in compliance with such laws and regulations; and
- (b) Inspecting correspondence, if any, with the relevant licensing or regulatory authorities.

27. As the financial reporting consequences of other laws and regulations can vary depending on the entity's operations, the internal audit procedures required by paragraph 26 are directed to bringing to the internal auditor's attention instances of non-compliance with laws and regulations that may have a significant impact on the functioning of the entity.

Non-Compliance brought to the Internal Auditor's Attention through Other Audit Procedures

28. During the internal audit, the internal auditor shall remain alert to the possibility that other audit procedures applied may bring instances of non-compliance or suspected non-compliance with laws and regulations to the internal auditor's attention. For example, such audit procedures may include:

- Reading minutes;
- Inquiring of the entity's management and in-house legal counsel or external legal counsel concerning litigation, claims and assessments; and
- Performing substantive tests of details of classes of transactions, account balances or disclosures.

Written Representations

29. The internal auditor shall request management and, where appropriate, those charged with governance to provide written representations that all known instances of non-compliance or suspected non-compliance with laws and regulations which impact the functioning of the entity, including the reporting framework, have been disclosed to the internal auditor.

30. Because the effect of non-compliance on the functioning of an entity can vary considerably, written representations provide necessary audit evidence about management's knowledge of identified or suspected non-compliance with

Standard on Internal Audit (SIA) 17

laws and regulations, whose effects may have a significant impact on the functioning of the entity. However, written representations do not provide sufficient appropriate audit evidence on their own and, accordingly, do not affect the nature and extent of other audit evidence that is to be obtained by the internal auditor.

Internal Audit Procedures When Non-Compliance is Not Identified or Suspected

31. In the absence of identified or suspected non-compliance, the internal auditor is not required to perform audit procedures regarding the entity's compliance with laws and regulations, other than those set out in paragraphs 22-30.

Internal Audit Procedures When Non-Compliance is Identified or Suspected

32. If the internal auditor becomes aware of information concerning an instance of non-compliance or suspected non-compliance with laws and regulations, the internal auditor shall obtain:

- (a) An understanding of the nature of the act and the circumstances in which it has occurred; and
- (b) Further information to evaluate the possible effect on the functioning of the entity.

Indications of Non-Compliance with Laws and Regulations

33. When the internal auditor becomes aware of the existence of, or information about, the following matters, it may be an indication of non-compliance with laws and regulations:

- Investigations by regulatory organisations and government departments or payment of fines or penalties.
- Payments for unspecified services or loans to consultants, related parties, employees or government employees.
- Sales commissions or agent's fees that appear excessive in relation to those ordinarily paid by the entity or in its industry or to the services actually

Consideration of Laws and Regulations in an Internal Audit

received.

- Purchasing at prices significantly above or below market price.
- Unusual payments in cash, purchases in the form of cashiers' cheques payable to bearer or transfers to numbered bank accounts.
- Unusual payments towards legal and retainership fees.
- Unusual transactions with companies registered in tax havens.
- Payments for goods or services made other than to the country from which the goods or services originated.
- Payments without proper exchange control documentation.
- Existence of an information system which fails, whether by design or by accident, to provide an adequate audit trail or sufficient evidence.
- Unauthorised transactions or improperly recorded transactions.
- Adverse media comment.

Matters Relevant to the Internal Auditor's Evaluation

34. Matters relevant to the internal auditor's evaluation of the possible effect on the entity's functioning include:

- The potential financial consequences of non-compliance with laws and regulations on the functioning of the entity including, for example, the imposition of fines, penalties, damages, threat of expropriation of assets, enforced discontinuation of operations and litigation.
- Whether the potential financial consequences need to be informed to the management for the limited objective of suitable disclosure.
- Whether the potential financial consequences are so serious as to call into question the ability of the entity to continue as a going concern.

35. The internal auditor may discuss the findings with those charged with governance where they may be able to provide additional audit evidence. For example, the internal auditor may confirm that those charged with governance have the same understanding of the facts and circumstances relevant to

Standard on Internal Audit (SIA) 17

transactions or events that have led to the possibility of non-compliance with laws and regulations.

36. If the internal auditor suspects there may be non-compliance, the internal auditor shall discuss the matter with management and, where appropriate, those charged with governance. If management or, as appropriate, those charged with governance do not provide sufficient information to the internal auditor that the entity is in fact in compliance with laws and regulations, the internal auditor may consider it appropriate to consult with the entity's in-house legal counsel or external legal counsel about the application of the laws and regulations to the circumstances, including the possibility of fraud, and the possible impact on the functioning of the entity. When it is not considered appropriate to consult with the entity's legal counsel or when the internal auditor is not satisfied with the legal counsel's opinion, the internal auditor may consider it appropriate to consult the internal auditor's own legal counsel as to whether a contravention of a law or regulation is involved, the possible legal consequences, including the possibility of fraud in accordance with the Standard on Internal Audit (SIA) 11, "Consideration of Fraud in an Internal Audit", and what further action, if any, the internal auditor would take.

37. If sufficient information about suspected non-compliance cannot be obtained, the internal auditor shall evaluate the effect of the lack of sufficient appropriate audit evidence on the internal auditor's observations and findings.

Evaluating the Implications of Non-Compliance

38. The internal auditor shall evaluate the implications of non-compliance in relation to other aspects of the internal audit, including the internal auditor's risk assessment and the reliability of written representations, and take appropriate action.

39. The implications of particular instances of non-compliance identified by the internal auditor will depend on the relationship of the perpetration and concealment, if any, of the act to specific control activities and the level of management or employees involved, especially implications arising from the involvement of the highest authority within the entity.

40. In exceptional cases, the internal auditor may consider whether, unless

Consideration of Laws and Regulations in an Internal Audit

prohibited by law or regulation, withdrawal from the engagement is necessary when management or those charged with governance do not take the remedial action that the internal auditor considers appropriate in the circumstances. When deciding whether withdrawal from the engagement is necessary, the internal auditor should consider whether there is an obligation, contractual or otherwise to report the circumstances necessitating the withdrawal to other parties.

Reporting of Identified or Suspected Non-Compliance

Reporting Non-Compliance to Those Charged with Governance

41. Unless all of those charged with governance are involved in management of the entity, and therefore are aware of matters involving identified or suspected non-compliance already communicated in accordance with the Standard on Internal Audit (SIA) 9, "Communication with Management", by the internal auditor, the internal auditor shall communicate with those charged with governance matters involving non-compliance with laws and regulations that come to the internal auditor's attention during the course of the internal audit, other than when the matters are clearly inconsequential.

42. If, in the internal auditor's judgment, the non-compliance referred to in paragraph 41 is believed to be intentional and material, the internal auditor shall communicate the matter to those charged with governance as soon as practicable.

Reporting Non-Compliance in the Internal Auditor's Report

43. If the internal auditor concludes that the non-compliance has a significant impact on the functioning of an entity and has not been adequately dealt with by the management, the internal auditor shall report the same in accordance with SIA 4, "Reporting".

44. If the internal auditor is precluded by management or those charged with governance from obtaining sufficient appropriate audit evidence to evaluate whether non-compliance that may be significant to the functioning of the entity has, or is likely to have, occurred, the internal auditor should report the same in accordance with SIA 4, "Reporting".

45. If the internal auditor is unable to determine whether non-compliance

Standard on Internal Audit (SIA) 17

has occurred because of limitations imposed by the circumstances rather than by management or those charged with governance, the internal auditor shall evaluate the effect on the internal auditor's observations and findings in accordance with SIA 4, "Reporting".

Documentation

46. The internal auditor shall document identified or suspected non-compliance with laws and regulations and the results of discussion with management and, where applicable, those charged with governance and other parties outside the entity in accordance with the Standard on Internal Audit (SIA) 3, "Documentation".

47. The internal auditor's documentation of findings regarding identified or suspected non-compliance with laws and regulations may include, for example:

- Copies of records or documents.
- Minutes of discussions held with management, those charged with governance or parties outside the entity.

Effective Date

48. This Standard on Internal Audit (SIA) is effective for all internal audits beginning on or after Earlier application of the SIA is encouraged.