

# INVITATION TO COMMENT ON THE EXPOSURE DRAFT OF AUDITING AND ASSURANCE STANDARD (AAS) XX, UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT

*The Auditing and Assurance Standards Board of the Institute of Chartered Accountants of India invites comments on the Exposure Draft of the proposed Auditing and Assurance Standard (AAS) XX, Understanding the Entity and its Environment and Assessing the Risk of Material Misstatements.*

**Comments are most helpful if they indicate the specific paragraph(s) to which they relate, contain a clear rationale and, where applicable, provide a suggestion for alternative wording.**

*Comments should be submitted in writing to the Secretary, Auditing and Assurance Standards Board, The Institute of Chartered Accountants of India, Post Box No. 7100, Indraprastha Marg, New Delhi – 110 002, so as to be received not later than **10<sup>th</sup> June 2005**. Comments can also be sent by e-mail at [aasb@icai.org](mailto:aasb@icai.org).*

---

## EXPOSURE DRAFT AUDITING AND ASSURANCE STANDARD (AAS) XX UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT AND ASSESSING THE RISKS OF MATERIAL MISSTATEMENT<sup>1</sup>

*The following is the text of the Auditing and Assurance Standard (AAS) XX, “Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement”, issued by the Council of the Institute of Chartered Accountants of India. This Standard should be read in conjunction with the “Preface to the Statements on Standard Auditing Practices”, issued by the Institute.<sup>2</sup>*

### Introduction

1. The purpose of this Auditing and Assurance Standard

(AAS) is to establish standards on obtaining an understanding of the entity and its environment, including its internal control, and on assessing the risks of material misstatement in an audit of financial statements. The importance of the auditor’s risk assessment as a basis for further audit procedures is discussed in AAS XXX, “The Auditor’s Procedures in Response to Assessed Risks”\*.

2. **The auditor should obtain an understanding of the entity and its environment, including its internal control, sufficient to identify and assess the risks of**

---

<sup>1</sup> The date this Auditing and Assurance Standard becomes effective, the following Auditing and Assurance Standards, issued by the Council of the Institute shall stand withdrawn:

- AAS 6, Risk Assessment and Internal Controls
- AAS 20, Knowledge of the Business
- AAS 29, Auditing in a Computer Information Systems Environment

<sup>2</sup> With the formation of the Auditing Practices Committee {now known as the Auditing and Assurance Standards Board} in 1982, the Council of the Institute has been issuing a series of Statements on Standard Auditing Practices (SAPs). SAPs have been renamed as Auditing and Assurance Standards (AASs). The Auditing and Assurance Standards (hitherto known as SAPs) lay down the principles governing an audit. These principles apply whenever an independent audit is carried out. Auditing and Assurance Standards become mandatory on the dates specified in the respective AAS. Their mandatory status implies that, while discharging their attest function, it will be the duty of the members of the Institute to ensure that the AASs are followed in the audit of financial information covered by their audit reports. If, for any reason, a member has not been able to perform an audit in accordance with the AASs, his report should draw attention to the material departures therefrom. The Auditing and Assurance Standards have the same authority as that attached to the Statements on Standard Auditing Practices.

\* The Exposure Draft of AAS XXX, “The Auditor’s Procedures in Response to Assessed Risks”, is published elsewhere in the Journal.

**material misstatement of the financial statements whether due to fraud or error, and sufficient to design and perform further audit procedures.** AAS 5, “Audit Evidence”, requires the auditor to use assertions in sufficient detail to form a basis for the assessment of risks of material misstatement and the design and performance of further audit procedures. This AAS requires the auditor to make risk assessments at the financial statement and assertion levels based on an appropriate understanding of the entity and its environment, including its internal control. It is the auditor’s responsibility to determine overall responses and to design and perform further audit procedures whose nature, timing, and extent are responsive to the risk assessments. The requirements of this AAS are to be applied in conjunction with the requirements of other Auditing and Assurance Standards. In particular, further requirements in relation to the auditor’s responsibility to assess the risks of material misstatement due to fraud is discussed in AAS 4, The Auditor’s Responsibility to Consider Fraud and Error in an Audit of Financial Statements.

3. The following is an overview of the requirements of this Standard:
  - Risk assessment procedures and sources of information about the entity and its environment, including its internal control. This section explains the audit procedures that the auditor is required to perform to obtain the understanding of the entity and its environment, including its internal control (risk assessment procedures). It also requires discussion among the engagement team about the susceptibility of the entity’s financial statements to material misstatement.
  - Understanding the entity and its environment, including its internal control. This section requires the auditor to understand specified aspects of the entity and its environment, and components of its internal control, in order to identify and assess the risks of material misstatement.
  - Assessing the risks of material misstatement. This section requires the auditor to identify and assess the risks of material misstatement at the financial statement and assertion levels. The auditor:
    - Identifies risks by considering the entity and its environment, including relevant controls, and by considering the classes of transactions, account balances, and disclosures in the financial statements;
    - Relates the identified risks to what can go wrong at the assertion level; and
    - Considers the significance and likelihood of the risks.
    - This section also requires the auditor to determine whether any of the assessed risks are significant risks that require special audit considera-

tion or risks for which substantive procedures alone do not provide sufficient appropriate audit evidence. The auditor is required to evaluate the design of the entity’s controls, including relevant control activities, over such risks and determine whether they have been implemented.

- Communicating with those charged with governance and management. This section deals with matters relating to internal control that the auditor communicates to those charged with governance and management.
  - Documentation. This section establishes related documentation requirements.
4. Obtaining an understanding of the entity and its environment is an essential aspect of performing an audit in accordance with Auditing and Assurance Standards. In particular, that understanding establishes a frame of reference within which the auditor plans the audit and exercises professional judgment about assessing risks of material misstatement of the financial statements and responding to those risks throughout the audit, for example when:
    - Establishing materiality and evaluating whether the judgment about materiality remains appropriate as the audit progresses;
    - Considering the appropriateness of the selection and application of accounting policies, and the adequacy of financial statement disclosures;
    - Identifying areas where special audit consideration may be necessary, for example, related party transactions, the appropriateness of management’s use of the going concern assumption, or considering the business purpose of transactions;
    - Developing benchmarks for use when performing analytical procedures;
    - Designing and performing further audit procedures to reduce audit risk to an acceptably low level; and
    - Evaluating the sufficiency and appropriateness of audit evidence obtained, such as the appropriateness of assumptions and of management’s oral and written representations.
  5. The auditor uses professional judgment to determine the extent of the understanding required of the entity and its environment, including its internal control. The auditor’s primary consideration is whether the understanding that has been obtained is sufficient to assess the risks of material misstatement of the financial statements and to design and perform further audit procedures. The depth of the overall understanding that is required by the auditor in performing the audit is less than that possessed by management in managing the entity.

**Risk Assessment Procedures and Sources of Information About the Entity and Its Environment, Including Its Internal Control**

6. Obtaining an understanding of the entity and its envi-

ronment, including its internal control, is a continuous, dynamic process of gathering, updating and analyzing information throughout the audit. Audit procedures to obtain an understanding are referred to as “risk assessment procedures” because some of the information obtained by performing such procedures may be used by the auditor as audit evidence to support assessments of the risks of material misstatement. In addition, in performing risk assessment procedures, the auditor may obtain audit evidence about classes of transactions, account balances, or disclosures and related assertions and about the operating effectiveness of controls. It is not, however, necessary that such audit procedures should have been specifically planned as substantive procedures or as tests of controls. The auditor also may choose to perform substantive procedures or tests of controls concurrently with risk assessment procedures because it is efficient to do so.

### Risk Assessment Procedures

**7. The auditor should perform the following risk assessment procedures to obtain an understanding of the entity and its environment, including its internal control:**

- (a) Inquiries of management and others within the entity;**
- (b) Analytical procedures; and**
- (c) Observation and inspection.**

The auditor is not required to perform all the risk assessment procedures described above for each aspect of the understanding described in paragraph 20. However, all the risk assessment procedures are performed by the auditor in the course of obtaining the required understanding.

8. In addition, the auditor performs other audit procedures where the information obtained may be helpful in identifying risks of material misstatement. For example, the auditor may consider making inquiries of the entity’s external legal counsel or of valuation experts that the entity has used. Reviewing information obtained from external sources such as reports by analysts, banks, or rating agencies; trade and economic journals; or regulatory or financial publications may also be useful in obtaining information about the entity.
9. Although much of the information the auditor obtains by inquiries can be obtained from management and those responsible for financial reporting, inquiries of others within the entity, such as production and internal audit personnel, and other employees with different levels of authority, may be useful in providing the auditor with a different perspective in identifying risks of material misstatement. In determining others within the entity to whom inquiries may be directed, and the extent of those inquiries, the auditor considers what information may be obtained that helps the auditor in identify-

ing risks of material misstatement. For example:

- Inquiries directed towards those charged with governance may help the auditor understand the environment in which the financial statements are prepared.
- Inquiries directed toward internal audit personnel may relate to their activities concerning the design and effectiveness of the entity’s internal control and whether management has satisfactorily responded to any findings from these activities.
- Inquiries of employees involved in initiating, processing or recording complex or unusual transactions may help the auditor in evaluating the appropriateness of the selection and application of certain accounting policies.
- Inquiries directed toward in-house legal counsel may relate to such matters as litigation, compliance with laws and regulations, knowledge of fraud or suspected fraud affecting the entity, warranties, post-sales obligations, arrangements (such as joint ventures) with business partners and the meaning of contract terms.
- Inquiries directed towards marketing or sales personnel may relate to changes in the entity’s marketing strategies, sales trends, or contractual arrangements with its customers.

10. Analytical procedures may be helpful in identifying the existence of unusual transactions or events, and amounts, ratios, and trends that might indicate matters that have financial statement and audit implications. In performing analytical procedures as risk assessment procedures, the auditor develops expectations about plausible relationships that are reasonably expected to exist. When comparison of those expectations with recorded amounts or ratios developed from recorded amounts yields unusual or unexpected relationships, the auditor considers those results in identifying risks of material misstatement. However, when such analytical procedures use data aggregated at a high level (which is often the situation), the results of those analytical procedures only provide a broad initial indication about whether a material misstatement may exist. Accordingly, the auditor considers the results of such analytical procedures along with other information gathered in identifying the risks of material misstatement. See AAS 14, “Analytical Procedures”, for additional detail on the use of analytical procedures.

11. Observation and inspection may support inquiries of management and others, and also provide information about the entity and its environment. Such audit procedures ordinarily include the following:

- Observation of entity activities and operations.
- Inspection of documents (such as business plans and strategies), records, and internal control manuals.
- Reading reports prepared by management (such as

## FOR YOUR INFORMATION

quarterly management reports and interim financial statements) and those charged with governance (such as minutes of board of directors meetings).

- Visits to the entity's premises and plant facilities.
- Tracing transactions through the information system relevant to financial reporting (walk-throughs).

**12. When the auditor intends to use information about the entity and its environment obtained in prior periods, the auditor should determine whether changes have occurred that may affect the relevance of such information in the current audit.** For continuing engagements, the auditor's previous experience with the entity contributes to the understanding of the entity. For example, audit procedures performed in previous audits ordinarily provide audit evidence about the entity's organizational structure, business and controls, as well as information about past misstatements and whether or not they were corrected on a timely basis, which assists the auditor in assessing risks of material misstatement in the current audit. However, such information may have been rendered irrelevant by changes in the entity or its environment. The auditor makes inquiries and performs other appropriate audit procedures, such as walk-throughs of systems, to determine whether changes have occurred that may affect the relevance of such information.

13. When relevant to the audit, the auditor also considers other information such as that obtained from the auditor's client acceptance or continuance process or, where practicable, experience gained on other engagements performed for the entity, for example, engagements to review interim financial information.

### Discussion Among the Engagement Team

**14. The members of the engagement team should discuss the susceptibility of the entity's financial statements to material misstatements.**

15. The objective of this discussion is for members of the engagement team to gain a better understanding of the potential for material misstatements of the financial statements resulting from fraud or error in the specific areas assigned to them, and to understand how the results of the audit procedures that they perform may affect other aspects of the audit including the decisions about the nature, timing, and extent of further audit procedures.

16. The discussion provides an opportunity for more experienced engagement team members, including the engagement partner, to share their insights based on their knowledge of the entity, and for the team members to exchange information about the business risks to which the entity is subject and about how and where the financial statements might be susceptible to material misstatement. As required by AAS 4, particular

emphasis is given to the susceptibility of the entity's financial statements to material misstatement due to fraud. The discussion also addresses application of the applicable financial reporting framework to the entity's facts and circumstances.

17. Professional judgment is used to determine which members of the engagement team are included in the discussion, how and when it occurs, and the extent of the discussion. The key members of the engagement team are ordinarily involved in the discussion; however, it is not necessary for all team members to have a comprehensive knowledge of all aspects of the audit. The extent of the discussion is influenced by the roles, experience, and information needs of the engagement team members. In a multi-location audit, for example, there may be multiple discussions that involve the key members of the engagement team in each significant location. Another factor to consider in planning the discussions is whether to include experts assigned to the engagement team. For example, the auditor may determine that including a professional possessing specialist information technology (IT) or other skills is needed on the engagement team and therefore includes that individual in the discussion. [IT encompasses automated means of originating, processing storing, and communicating information, and includes recording devices, communication systems, computer systems (including hardware and software components and data), and other electronic devices].

18. The auditor plans and performs the audit with an attitude of professional skepticism. The discussion among the engagement team members emphasizes the need to maintain professional skepticism throughout the engagement, to be alert for information or other conditions that indicate that a material misstatement due to fraud or error may have occurred, and to be rigorous in following up on such indications.

19. Depending on the circumstances of the audit, there may be further discussions in order to facilitate the ongoing exchange of information between engagement team members regarding the susceptibility of the entity's financial statements to material misstatements. The purpose is for engagement team members to communicate and share information obtained throughout the audit that may affect the assessment of the risks of material misstatement due to fraud or error or the audit procedures performed to address the risks.

### Understanding the Entity and its Environment, Including its Internal Control

20. The auditors' understanding of the entity and its environment consists of an understanding of the following aspects:

- (a) Industry, regulatory, and other external factors,

including the applicable financial reporting framework.

- (b) Nature of the entity, its governance and organizational structure;
- (c) Entity's selection and application of accounting policies.
- (d) Objectives and strategies and the related business risks that may result in a material misstatement of the financial statements.
- (e) Measurement and review of the entity's financial performance.
- (f) Internal control.

**Appendix 1** contains examples of matters that the auditor may consider in obtaining an understanding of the entity and its environment relating to categories (a) through (d) above. **Appendix 2** contains a detailed explanation of the internal control components.

21. The nature, timing, and extent of the risk assessment procedures performed depend on the circumstances of the engagement such as the size and complexity of the entity and the auditor's experience with it. In addition, identifying significant changes in any of the above aspects of the entity from prior periods is particularly important in gaining a sufficient understanding of the entity to identify and assess risks of material misstatement.

### Industry, Regulatory and Other External Factors, Including the Applicable Financial Reporting Framework

22. **The auditor should obtain an understanding of relevant industry, regulatory, and other external factors including the applicable financial reporting framework.** These factors include industry conditions such as the competitive environment, supplier and customer relationships, and technological developments; the regulatory environment encompassing, among other matters, the applicable financial reporting framework, the legal and political environment, and environmental requirements affecting the industry and the entity; and other external factors such as general economic conditions. See AAS 21, Consideration of Laws and Regulations in an Audit of Financial Statements for additional requirements related to the legal and regulatory framework applicable to the entity and the industry.
23. The industry in which the entity operates may give rise to specific risks of material misstatement arising from the nature of the business or the degree of regulation. For example, long-term contracts may involve significant estimates of revenues and costs that give rise to risks of material misstatement. In such cases, the auditor considers whether the engagement team includes members with sufficient relevant knowledge and experience.
24. Legislative and regulatory requirements often deter-

mine the applicable financial reporting framework to be used by management in preparing the entity's financial statements. In most cases, the applicable financial reporting framework will be that of the jurisdiction in which the entity is registered or operates and in which the auditor is based, and the auditor and the entity will have a common understanding of that framework.

### Nature of the Entity

25. **The auditor should obtain an understanding of the nature of the entity.** The nature of an entity refers to the entity's operations, its ownership and governance, the types of investments that it is making and plans to make, the way that the entity is structured and how it is financed. An understanding of the nature of an entity enables the auditor to understand the classes of transactions, account balances, and disclosures to be expected in the financial statements.
26. The entity may have a complex structure with subsidiaries or other components in multiple locations. In addition to the difficulties of consolidation in such cases, other issues with complex structures that may give rise to risks of material misstatement include: the allocation of goodwill to business segments, and its impairment; whether investments are joint ventures, subsidiaries, or investments accounted for using the equity method; and whether special-purpose entities are accounted for appropriately.
27. An understanding of the ownership and relations between owners and other people or entities is also important in determining whether related party transactions have been identified and accounted for appropriately. AAS 23, Related Parties provides additional guidance on the auditor's considerations relevant to related parties.
28. **The auditor should obtain an understanding of the entity's selection and application of accounting policies and consider whether they are appropriate for its business and consistent with the applicable financial reporting framework and accounting policies used in the relevant industry.** The understanding encompasses the methods the entity uses to account for significant and unusual transactions; the effect of significant accounting policies in controversial or emerging areas for which there is a lack of authoritative guidance or consensus; and changes in the entity's accounting policies. The auditor also identifies financial reporting standards and regulations that are new to the entity and considers when and how the entity will adopt such requirements. Where the entity has changed its selection of or method of applying a significant accounting policy, the auditor considers the reasons for the change and whether it is appropriate and consistent with the requirements of the applicable financial reporting framework.

29. The presentation of financial statements in conformity with the applicable financial reporting framework includes adequate disclosure of material matters. These matters relate to the form, arrangement, and content of the financial statements and their appended notes, including, for example, the terminology used, the amount of detail given, the classification of items in the statements, and the basis of amounts set forth. The auditor considers whether the entity has disclosed a particular matter appropriately in light of the circumstances and facts of which the auditor is aware at the time.

### Objectives and Strategies and Related Business Risks

**30. The auditor should obtain an understanding of the entity's objectives and strategies, and the related business risks that may result in material misstatement of the financial statements.** The entity conducts its business in the context of industry, regulatory and other internal and external factors. To respond to these factors, the entity's management or those charged with governance define objectives, which are the overall plans for the entity. Strategies are the operational approaches by which management intends to achieve its objectives. Business risks result from significant conditions, events, circumstances, actions or inactions that could adversely affect the entity's ability to achieve its objectives and execute its strategies, or through the setting of inappropriate objectives and strategies. Just as the external environment changes, the conduct of the entity's business is also dynamic and the entity's strategies and objectives change over time.

31. Business risk is broader than the risk of material misstatement of the financial statements, though it includes the latter. Business risk particularly may arise from change or complexity, though a failure to recognize the need for change may also give rise to risk. Change may arise, for example, from the development of new products that may fail; from an inadequate market, even if successfully developed; or from flaws that may result in liabilities and reputational risk. An understanding of business risks increases the likelihood of identifying risks of material misstatement. However, the auditor does not have a responsibility to identify or assess all business risks.

32. Most business risks will eventually have financial consequences and, therefore, an effect on the financial statements. However, not all business risks give rise to risks of material misstatement. A business risk may have an immediate consequence for the risk of misstatement for classes of transactions, account balances, and disclosures at the assertion level or the financial statements as a whole. For example, the business risk arising from a contracting customer base due to industry consolidation may increase the risk of misstatement

associated with the valuation of receivables. However, the same risk, particularly in combination with a contracting economy, may also have a longer-term consequence, which the auditor considers when assessing the appropriateness of the going concern assumption. The auditor's consideration of whether a business risk may result in material misstatement is, therefore, made in light of the entity's circumstances. Examples of conditions and events that may indicate risks of material misstatement are given in [Appendix 3](#).

33. Usually management identifies business risks and develops approaches to address them. Such a risk assessment process is part of internal control and is discussed in paragraphs 76-79.

34. Smaller entities often do not set their objectives and strategies, or manage the related business risks, through formal plans or processes. In many cases there may be no documentation of such matters. In such entities, the auditor's understanding is ordinarily obtained through inquiries of management and observation of how the entity responds to such matters.

### Measurement and Review of the Entity's Financial Performance

**35. The auditor should obtain an understanding of the measurement and review of the entity's financial performance.** Performance measures and their review indicate to the auditor aspects of the entity's performance that management and others consider to be of importance. Performance measures, whether external or internal, create pressures on the entity that, in turn, may motivate management to take action to improve the business performance or to misstate the financial statements. Obtaining an understanding of the entity's performance measures assists the auditor in considering whether such pressures result in management actions that may have increased the risks of material misstatement.

36. Management's measurement and review of the entity's financial performance is to be distinguished from the monitoring of controls (discussed as a component of internal control in paragraphs 96-99), though their purposes may overlap. Monitoring of controls, however, is specifically concerned with the effective operation of internal control through consideration of information about the control. The measurement and review of performance is directed at whether business performance is meeting the objectives set by management (or third parties), but in some cases performance indicators also provide information that enables management to identify deficiencies in internal control.

37. Internally-generated information used by management for this purpose may include key performance indicators (financial and non-financial), budgets, variance analy-

## FOR YOUR INFORMATION

sis, segment information and divisional, departmental or other level performance reports, and comparisons of an entity's performance with that of competitors. External parties may also measure and review the entity's financial performance. For example, external information such as analysts reports and credit rating agency reports may provide information useful to the auditor's understanding of the entity and its environment. Such reports may be obtained from the entity being audited.

38. Internal measures may highlight unexpected results or trends requiring management's inquiry of others in order to determine their cause and take corrective action (including, in some cases, the detection and correction of misstatements on a timely basis). Performance measures may also indicate to the auditor a risk of misstatement of related financial statement information. For example, performance measures may indicate that the entity has unusually rapid growth or profitability when compared to that of other entities in the same industry. Such information, particularly if combined with other factors such as performance-based bonus or incentive remuneration, may indicate the potential risk of management bias in the preparation of the financial statements.
39. Much of the information used in performance measurement may be produced by the entity's information system. If management assumes that data used for reviewing the entity's performance are accurate without having a basis for that assumption, errors may exist in the information, potentially leading management to incorrect conclusions about performance. When the auditor intends to make use of the performance measures for the purpose of the audit (for example, for analytical procedures), the auditor considers whether the information related to management's review of the entity's performance provides a reliable basis and is sufficiently precise for such a purpose. If making use of performance measures, the auditor considers whether they are precise enough to detect material misstatements.
40. Smaller entities ordinarily do not have formal processes to measure and review the entity's financial performance. Management nevertheless often relies on certain key indicators which knowledge and experience of the business suggest are reliable bases for evaluating financial performance and taking appropriate action.

### Internal Control

41. **The auditor should obtain an understanding of internal control relevant to the audit.** The auditor uses the understanding of internal control to identify types of potential misstatements, consider factors that affect the risks of material misstatement, and design the nature, timing, and extent of further audit procedures. Internal control relevant to the audit is discussed in paragraphs 47-53 below. In addition, the depth of the

understanding is discussed in paragraphs 54-56 below.

42. Internal control is the process designed and effected by those charged with governance, management, and other personnel to provide reasonable assurance about the achievement of the entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations and compliance with applicable laws and regulations. It follows that internal control is designed and implemented to address identified business risks that threaten the achievement of any of these objectives.
43. Internal control, as discussed in this AAS, consists of the following components:
  - (a) The control environment.
  - (b) The entity's risk assessment process.
  - (c) The information system, including the related business processes, relevant to financial reporting, and communication.
  - (d) Control activities.
  - (e) Monitoring of controls.

**Appendix 2** contains a detailed discussion of the internal control components.

44. The division of internal control into the five components provides a useful framework for auditors to consider how different aspects of an entity's internal control may affect the audit. The division does not necessarily reflect how an entity considers and implements internal control. Also, the auditor's primary consideration is whether, and how, a specific control prevents, or detects and corrects, material misstatements in classes of transactions, account balances, or disclosures, and their related assertions, rather than its classification into any particular component. Accordingly, auditors may use different terminology or frameworks to describe the various aspects of internal control, and their effect on the audit than those used in this Standard provided all the components described in this AAS are addressed.
45. The way in which internal control is designed and implemented varies with an entity's size and complexity. Specifically, smaller entities may use less formal means and simpler processes and procedures to achieve their objectives. For example, smaller entities with active management involvement in the financial reporting process may not have extensive descriptions of accounting procedures or detailed written policies. For some entities, in particular very small entities, the owner-manager (i.e. the proprietors of entities who are involved in the running of the entity on a day to day basis) may perform functions which in a larger entity would be regarded as belonging to several of the components of internal control. Therefore, the components of internal control may not be clearly distinguished within smaller entities, but their underlying purposes are equally valid.

46. For the purposes of this AAS, the term “internal control” encompasses all five components of internal control stated above. In addition, the term “controls” refers to one or more of the components, or any aspect thereof.

### Controls Relevant to the Audit

47. There is a direct relationship between an entity’s objectives and the controls it implements to provide reasonable assurance about their achievement. The entity’s objectives, and therefore controls, relate to financial reporting, operations and compliance; however, not all of these objectives and controls are relevant to the auditor’s risk assessment.
48. Ordinarily, controls that are relevant to an audit pertain to the entity’s objective of preparing financial statements for external purposes that give a true and fair view (or are presented fairly, in all material respects) in accordance with the applicable financial reporting framework and the management of risk that may give rise to a material misstatement in those financial statements. It is a matter of the auditor’s professional judgment, subject to the requirements of this AAS, whether a control, individually or in combination with others, is relevant to the auditor’s considerations in assessing the risks of material misstatement and designing and performing further procedures in response to assessed risks. In exercising that judgment, the auditor considers the circumstances, the applicable component and factors such as the following:
- The auditor’s judgment about materiality.
  - The size of the entity.
  - The nature of the entity’s business, including its organization and ownership characteristics.
  - The diversity and complexity of the entity’s operations.
  - Applicable legal and regulatory requirements.
  - The nature and complexity of the systems that are part of the entity’s internal control, including the use of service organizations.
49. Controls over the completeness and accuracy of information produced by the entity may also be relevant to the audit if the auditor intends to make use of the information in designing and performing further procedures. The auditor’s previous experience with the entity and information obtained in understanding the entity and its environment and throughout the audit assists the auditor in identifying controls relevant to the audit. Further, although internal control applies to the entire entity or to any of its operating units or business processes, an understanding of internal control relating to each of the entity’s operating units and business processes may not be relevant to the audit.
50. Controls relating to operations and compliance objectives may, however, be relevant to an audit if they pertain

to data the auditor evaluates or uses in applying audit procedures. For example, controls pertaining to non-financial data that the auditor uses in analytical procedures, such as production statistics, or controls pertaining to detecting non-compliance with laws and regulations that may have a direct and material effect on the financial statements, such as controls over compliance with income tax laws and regulations used to determine the income tax provision, may be relevant to an audit.

51. An entity generally has controls relating to objectives that are not relevant to an audit and therefore need not be considered. For example, an entity may rely on a sophisticated system of automated controls to provide efficient and effective operations (such as a commercial airline’s system of automated controls to maintain flight schedules), but these controls ordinarily would not be relevant to the audit.
52. Internal control over safeguarding of assets against unauthorized acquisition, use, or disposition may include controls relating to financial reporting and operations objectives. In obtaining an understanding of each of the components of internal control, the auditor’s consideration of safeguarding controls is generally limited to those relevant to the reliability of financial reporting. For example, use of access controls, such as passwords, that limit access to the data and programs that process cash disbursements may be relevant to a financial statement audit. Conversely, controls to prevent the excessive use of materials in production generally are not relevant to a financial statement audit.
53. Controls relevant to the audit may exist in any of the components of internal control and a further discussion of controls relevant to the audit is included under the heading of each internal control component below. In addition, paragraphs 113 and 115 discuss certain risks for which the auditor is required to evaluate the design of the entity’s controls over such risks and determine whether they have been implemented.

### Depth of Understanding of Internal Control

54. Obtaining an understanding of internal control involves evaluating the design of a control and determining whether it has been implemented. Evaluating the design of a control involves considering whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements. Further explanation is contained in the discussion of each internal control component below. Implementation of a control means that the control exists and that the entity is using it. The auditor considers the design of a control in determining whether to consider its implementation. An improperly designed control may represent a material weakness (i.e. a weakness that could have a material effect on the

## FOR YOUR INFORMATION

financial statements) in the entity's internal control and the auditor considers whether to communicate this to those charged with governance and management as required by paragraph 120.

55. Risk assessment procedures to obtain audit evidence about the design and implementation of relevant controls may include inquiring of entity personnel, observing the application of specific controls, inspecting documents and reports, and tracing transactions through the information system relevant to financial reporting. Inquiry alone is not sufficient to evaluate the design of a control relevant to an audit and to determine whether it has been implemented.
56. Obtaining an understanding of an entity's controls is not sufficient to serve as testing the operating effectiveness of controls, unless there is some automation that provides for the consistent application of the operation of the control (manual and automated elements of internal control relevant to the audit are further described below). For example, obtaining audit evidence about the implementation of a manually operated control at a point in time does not provide audit evidence about the operating effectiveness of the control at other times during the period under audit. However, IT enables an entity to process large volumes of data consistently and enhances the entity's ability to monitor the performance of control activities and to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems. Therefore, because of the inherent consistency of IT processing, performing audit procedures to determine whether an automated control has been implemented may serve as a test of that control's operating effectiveness, depending on the auditor's assessment and testing of controls such as those over program changes. Tests of the operating effectiveness of controls are further described in AAS XXX.

### Characteristics of Manual and Automated Elements of Internal Control Relevant to the Auditor's Risk Assessment

57. Most entities make use of IT systems for financial reporting and operational purposes. However, even when IT is extensively used, there will be manual elements to the systems. The balance between manual and automated elements varies. In certain cases, particularly smaller, less complex entities, the systems may be primarily manual. In other cases, the extent of automation may vary with some systems substantially automated with few related manual elements and others, even within the same entity, predominantly manual. As a result, an entity's system of internal control is likely to contain manual and automated elements, the characteristics of which are relevant to the auditor's risk assessment and further audit procedures based thereon.

58. The use of manual or automated elements in internal control also affects the manner in which transactions are initiated, recorded, processed, and reported. [Paragraph 9 of Appendix 2 defines initiation, recording, processing, and reporting as used throughout this AAS.] Controls in a manual system may include such procedures as approvals and reviews of activities, and reconciliations and follow-up of reconciling items. Alternatively, an entity may use automated procedures to initiate, record, process, and report transactions, in which case records in electronic format replace such paper documents as purchase orders, invoices, shipping documents, and related accounting records. Controls in IT systems consist of a combination of automated controls (for example, controls embedded in computer programs) and manual controls. Further, manual controls may be independent of IT, may use information produced by IT, or may be limited to monitoring the effective functioning of IT and of automated controls, and to handling exceptions. When IT is used to initiate, record, process or report transactions, or other financial data for inclusion in financial statements, the systems and programs may include controls related to the corresponding assertions for material accounts or may be critical to the effective functioning of manual controls that depend on IT. An entity's mix of manual and automated controls varies with the nature and complexity of the entity's use of IT.
59. Generally, IT provides potential benefits of effectiveness and efficiency for an entity's internal control because it enables an entity to:
- Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data;
  - Enhance the timeliness, availability, and accuracy of information;
  - Facilitate the additional analysis of information;
  - Enhance the ability to monitor the performance of the entity's activities and its policies and procedures;
  - Reduce the risk that controls will be circumvented; and
  - Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.
60. IT also poses specific risks to an entity's internal control, including the following:
- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
  - Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.
  - The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned

## FOR YOUR INFORMATION

- duties thereby breaking down segregation of duties.
  - Unauthorized changes to data in master files.
  - Unauthorized changes to systems or programs.
  - Failure to make necessary changes to systems or programs.
  - Inappropriate manual intervention.
  - Potential loss of data or inability to access data as required.
61. Manual aspects of systems may be more suitable where judgment and discretion are required such as for the following circumstances:
- Large, unusual or non-recurring transactions.
  - Circumstances where errors are difficult to define, anticipate or predict.
  - In changing circumstances that require a control response outside the scope of an existing automated control.
  - In monitoring the effectiveness of automated controls.
62. Manual controls are performed by people, and therefore pose specific risks to the entity's internal control. Manual controls may be less reliable than automated controls because they can be more easily bypassed, ignored, or overridden and they are also more prone to simple errors and mistakes. Consistency of application of a manual control element cannot therefore be assumed. Manual systems may be less suitable for the following:
- High volume or recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented or detected by control parameters that are automated.
  - Control activities where the specific ways to perform the control can be adequately designed and automated.
63. The extent and nature of the risks to internal control vary depending on the nature and characteristics of the entity's information system. Therefore in understanding internal control, the auditor considers whether the entity has responded adequately to the risks arising from the use of IT or manual systems by establishing effective controls.

### Limitations of Internal Control

64. Internal control, no matter how well designed and operated, can provide an entity with only reasonable assurance about achieving the entity's financial reporting objectives. The likelihood of achievement is affected by limitations inherent to internal control. These include the realities that human judgment in decision-making can be faulty and that breakdowns in internal control can occur because of human failures, such as simple errors or mistakes. For example, if an entity's information system personnel do not completely understand how an order entry system processes sales transactions,

they may erroneously design changes to the system to process sales for a new line of products. On the other hand, such changes may be correctly designed but misunderstood by individuals who translate the design into program code. Errors also may occur in the use of information produced by IT. For example, automated controls may be designed to report transactions over a specified amount for management review, but individuals responsible for conducting the review may not understand the purpose of such reports and, accordingly, may fail to review them or investigate unusual items.

65. Additionally, controls can be circumvented by the collusion of two or more people or inappropriate management override of internal control. For example, management may enter into side agreements with customers that alter the terms and conditions of the entity's standard sales contracts, which may result in improper revenue recognition. Also, edit checks in a software program that are designed to identify and report transactions that exceed specified credit limits may be overridden or disabled.
66. Smaller entities often have fewer employees which may limit the extent to which segregation of duties is practicable. However, for key areas, even in a very small entity, it can be practicable to implement some degree of segregation of duties or other form of unsophisticated but effective controls. The potential for override of controls by the owner-manager depends to a great extent on the control environment and in particular, the owner-manager's attitudes about the importance of internal control.

### Control Environment

67. **The auditor should obtain an understanding of the control environment.** The control environment includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance and management concerning the entity's internal control and its importance in the entity. The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for effective internal control, providing discipline and structure.
68. The primary responsibility for the prevention and detection of fraud and error rests with both those charged with governance and the management of an entity. In evaluating the design of the control environment and determining whether it has been implemented, the auditor understands how management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behaviour, and established appropriate controls to prevent and detect fraud and error within the entity.
69. In evaluating the design of the entity's control environment, the auditor considers the following elements and how they have been incorporated into the entity's processes:

## FOR YOUR INFORMATION

- (a) Communication and enforcement of integrity and ethical values – essential elements which influence the effectiveness of the design, administration and monitoring of controls.
  - (b) Commitment to competence – management’s consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.
  - (c) Participation by those charged with governance – independence from management, their experience and stature, the extent of their involvement and scrutiny of activities, the information they receive, the degree to which difficult questions are raised and pursued with management and their interaction with internal and external auditors.
  - (d) Management’s philosophy and operating style – management’s approach to taking and managing business risks, and management’s attitudes and actions toward financial reporting, information processing and accounting functions and personnel.
  - (e) Organizational structure – the framework within which an entity’s activities for achieving its objectives are planned, executed, controlled and reviewed.
  - (f) Assignment of authority and responsibility – how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established.
  - (g) Human resource policies and practices – recruitment, orientation, training, evaluating, counseling, promoting, compensating and remedial actions.
70. In understanding the control environment elements, the auditor also considers whether they have been implemented. Ordinarily, the auditor obtains relevant audit evidence through a combination of inquiries and other risk assessment procedures, such as, corroborating inquiries through observation or inspection of documents. For example, through inquiries of management and employees, the auditor may obtain an understanding of how management communicates to employees its views on business practices and ethical behaviour. The auditor determines whether controls have been implemented by considering, for example, whether management has established a formal code of conduct and whether it acts in a manner that supports the code or condones violations of, or authorizes exceptions to the code.
71. Audit evidence for elements of the control environment may not be available in documentary form, in particular for smaller entities where communication between management and other personnel may be informal, yet effective. For example, management’s commitment to ethical values and competence are often implemented through the behaviour and attitude they demonstrate in managing the entity’s business instead of in a written code of conduct. Consequently, management’s attitudes, awareness and actions are of particular importance in the design of a smaller entity’s control environment. In addition, the role of those charged with governance is often undertaken by the owner-manager where there are no other owners.
72. The overall responsibilities of those charged with governance are recognized in codes of practice and other regulations or guidance produced for the benefit of those charged with governance. It is one, but not the only, role of those charged with governance to counterbalance pressures on management in relation to financial reporting. For example, the basis for management remuneration may place stress on management arising from the conflicting demands of fair reporting and the perceived benefits of improved results. In understanding the design of the control environment, the auditor considers such matters as the independence of the directors and their ability to evaluate the actions of management. The auditor also considers whether there is an audit committee that understands the entity’s business transactions and evaluates whether the financial statements give a true and fair view (or are presented fairly, in all material respects) in accordance with the applicable financial reporting framework.
73. The nature of an entity’s control environment is such that it has a pervasive effect on assessing the risks of material misstatement. For example, owner-manager controls may mitigate a lack of segregation of duties in a small business, or an active and independent board of directors may influence the philosophy and operating style of senior management in larger entities. The auditor’s evaluation of the design of the entity’s control environment includes considering whether the strengths in the control environment elements collectively provide an appropriate foundation for the other components of internal control, and are not undermined by control environment weaknesses. For example, human resource policies and practices directed toward hiring competent financial, accounting, and IT personnel may not mitigate a strong bias by top management to overstate earnings. Changes in the control environment may affect the relevance of information obtained in prior audits. For example, management’s decision to commit additional resources for training and awareness of financial reporting activities may reduce the risk of errors in processing financial information. Alternatively, management’s failure to commit sufficient resources to address security risks presented by IT may adversely affect internal control by allowing improper changes to be made to computer programs or to data, or by allowing unauthorized transactions to be processed.
74. The existence of a satisfactory control environment can be a positive factor when the auditor assesses the risks of material misstatement the nature, timing, and extent of the auditor’s further procedures. In particular, it may help reduce the risk of fraud, although a satisfactory control

## FOR YOUR INFORMATION

environment is not an absolute deterrent to fraud. Conversely, weaknesses in the control environment may undermine the effectiveness of controls and therefore be negative factors in the auditor's assessment of the risks of material misstatement, in particular in relation to fraud.

75. The control environment in itself does not prevent, or detect and correct, a material misstatement in classes of transactions, account balances, and disclosures and related assertions. The auditor, therefore, ordinarily considers the effect of other components along with the control environment when assessing the risks of material misstatement; for example, the monitoring of controls and the operation of specific control activities.

### The Entity's Risk Assessment Process

76. **The auditor should obtain an understanding of the entity's process for identifying business risks relevant to financial reporting objectives and deciding about actions to address those risks, and the results thereof.** The process is described as the "entity's risk assessment process" and forms the basis for how management determines the risks to be managed.
77. In evaluating the design and implementation of the entity's risk assessment process, the auditor determines how management identifies business risks relevant to financial reporting, estimates the significance of the risks, assesses the likelihood of their occurrence, and decides upon actions to manage them. If the entity's risk assessment process is appropriate to the circumstances, it assists the auditor in identifying risks of material misstatement.
78. The auditor inquires about business risks that management has identified and considers whether they may result in material misstatement. During the audit, the auditor may identify risks of material misstatement that management failed to identify. In such cases, the auditor considers whether there was an underlying risk of a kind that should have been identified by the entity's risk assessment process, and if so, why that process failed to do so and whether the process is appropriate to its circumstances. If, as a result, the auditor judges that there is a material weakness in the entity's risk assessment process, the auditor communicates to those charged with governance as required by paragraph 120.
79. In a smaller entity, management may not have a formal risk assessment process as described in paragraph 76. For such entities, the auditor discusses with management how risks to the business are identified by management and how they are addressed.

### Information System, Including the Related Business Processes, Relevant to Financial Reporting, and Communication

80. The information system relevant to financial reporting objectives, which includes the accounting system, con-

sists of the procedures and records established to initiate, record, process, and report entity transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity.

81. **The auditor should obtain an understanding of the information system, including the related business processes, relevant to financial reporting, including the following areas:**

- **The classes of transactions in the entity's operations that are significant to the financial statements.**
- **The procedures, within both IT and manual systems, by which those transactions are initiated, recorded, processed and reported in the financial statements.**
- **The related accounting records, whether electronic or manual, supporting information, and specific accounts in the financial statements, in respect of initiating, recording, processing and reporting transactions.**
- **How the information system captures events and conditions, other than classes of transactions that are significant to the financial statements.**
- **The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.**

82. In obtaining this understanding, the auditor considers the procedures used to transfer information from transaction processing systems to general ledger or financial reporting systems. The auditor also understands the entity's procedures to capture information relevant to financial reporting for events and conditions other than transactions, such as the depreciation and amortization of assets and changes in the recoverability of accounts receivables.

83. An entity's information system typically includes the use of standard journal entries that are required on a recurring basis to record transactions such as sales, purchases, and cash disbursements in the general ledger, or to record accounting estimates that are periodically made by management, such as changes in the estimate of uncollectible accounts receivable.

84. An entity's financial reporting process also includes the use of non-standard journal entries to record non-recurring, unusual transactions or adjustments. Examples of such entries include consolidating adjustments and entries for a business combination or disposal or non-recurring estimates such as an asset impairment. In manual, paper-based general ledger systems, non-standard journal entries may be identified through inspection of ledgers, journals, and supporting documentation. However, when automated procedures are used to maintain the general ledger and prepare financial statements, such Journal entries may exist only in electronic form and may be more easily identified through the use of computer-assisted audit techniques.

## FOR YOUR INFORMATION

85. Financial statements of the entity need to comply with the disclosure requirements laid down in the applicable financial reporting framework. For this, it is essential that the procedures involved in the preparation of financial statements should be so designed that the relevant information is accumulated, recorded, processed, summarized and appropriately reported in the financial statements.
86. In obtaining an understanding, the auditor considers risks of material misstatement associated with inappropriate override of controls over journal entries and the controls surrounding non-standard journal entries. For example, automated processes and controls may reduce the risk of inadvertent error but do not overcome the risk that individuals may inappropriately override such automated processes, say, by changing the amounts being automatically passed to the general ledger or financial reporting system. Furthermore, the auditor maintains an awareness that when IT is used to transfer information automatically, there may be little or no visible evidence of such intervention in the information systems.
87. The auditor also understands how the incorrect processing of transactions is resolved, for example, whether there is an automated suspense file and how it is used by the entity to ensure that suspense items are cleared out on a timely basis, and how system overrides or bypasses to controls are processed and accounted for.
88. The auditor obtains an understanding of the entity's information system relevant to financial reporting in a manner that is appropriate to the entity's circumstances. This includes obtaining an understanding of how transactions originate within the entity's business processes. An entity's business processes are the activities designed to develop, purchase, produce, sell and distribute an entity's products and services; ensure compliance with laws and regulations; and record information, including accounting and financial reporting information.
- 89. The auditor should understand how the entity communicates financial reporting roles and responsibilities and significant matters relating to financial reporting.** Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting and may take such forms as policy manuals and financial reporting manuals. It includes the extent to which personnel understand how their activities in the financial reporting information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity. Open communication channels help ensure that exceptions are reported and acted on. The auditor's understanding of communication pertaining to financial reporting matters also includes communications between management and those charged with governance, particularly the audit committee, as well as external communications such as those with regulatory authorities.
- Control Activities**
- 90. The auditor should obtain a sufficient understanding of control activities to assess the risks of material misstatement at the assertion level and to design further audit procedures responsive to assessed risks.** Control activities are the policies and procedures that help ensure that management directives are carried out; for example, that necessary actions are taken to address risks that threaten the achievement of the entity's objectives. Control activities, whether within IT or manual systems, have various objectives and are applied at various organizational and functional levels. Examples of specific control activities include those relating to the following:
- Authorization.
  - Performance reviews
  - Information processing
  - Physical controls
  - Segregation of duties
91. In obtaining an understanding of control activities, the auditor's primary consideration is whether, and how, a specific control activity, individually or in combination with others, prevents, or detects and corrects, material misstatements in classes of transactions, account balances, or disclosures. Control activities relevant to the audit are those for which the auditor considers it necessary to obtain an understanding in order to assess risks of material misstatement at the assertion level and to design and perform further audit procedures responsive to the assessed risks. An audit does not require an understanding of all the control activities related to each significant class of transactions, account balance, and disclosure in the financial statements or to every assertion relevant to them. The auditor's emphasis is on identifying and obtaining an understanding of control activities that address the areas where the auditor considers that material misstatements are more likely to occur. When multiple control activities achieve the same objective, it is unnecessary to obtain an understanding of each of the control activities related to such objective.
92. The auditor considers the knowledge about the presence or absence of control activities obtained from the understanding of the other components of internal control in determining whether it is necessary to devote additional attention to obtaining an understanding of control activities. In considering whether control activities are relevant to the audit, the auditor considers the risks the auditor has identified that may give rise to material misstatement. Also, control activities are relevant to the audit if the auditor is required to evaluate them as discussed in paragraphs 113 and 115.
- 93. The auditor should obtain an understanding of how the entity has responded to risks arising from IT.** The use of

IT affects the way that control activities are implemented. The auditor considers whether the entity has responded adequately to the risks arising from IT by establishing effective general IT-controls and application controls. From the auditor's perspective, controls over IT systems are effective when they maintain the integrity of information and the security of the data such systems process.

94. General IT-controls are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General IT-controls that maintain the integrity of information and security of data commonly include controls over the following:
- Data centre and network operations.
  - System software acquisition, change and maintenance.
  - Access security.
  - Application system acquisition, development, and maintenance.

They are generally implemented to deal with the risks referred to in paragraph 60 above.

95. Application controls are manual or automated procedures that typically operate at a business process level. Application controls can be preventative or detective in nature and are designed to ensure the integrity of the accounting records. Accordingly, application controls relate to procedures used to initiate, record, process and report transactions or other financial data. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. Examples include edit checks of input data, and numerical sequence checks with manual follow-up of exception reports or correction at the point of data entry.

### Monitoring of Controls

96. **The auditor should obtain an understanding of the major types of activities that the entity uses to monitor internal control over financial reporting, including those related to the control activities relevant to the audit, and how the entity initiates corrective actions to its controls.**
97. Monitoring of controls is a process to assess the effectiveness of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions modified for changes in conditions. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory activities.
98. In many entities, internal auditors or personnel performing similar functions contribute to the monitoring of an entity's

activities. See AAS 7, "Relying upon the Work of an Internal Auditor" for additional guidance. Management's monitoring activities may also include using information from communications from external parties such as customer complaints and regulator comments that may indicate problems or highlight areas in need of improvement.

99. Much of the information used in monitoring may be produced by the entity's information system. If management assumes that data used for monitoring are accurate without having a basis for that assumption, errors may exist in the information, potentially leading management to incorrect conclusions from its monitoring activities. The auditor obtains an understanding of the sources of the information related to the entity's monitoring activities, and the basis upon which management considers the information to be sufficiently reliable for the purpose. When the auditor intends to make use of the entity's information produced for monitoring activities, such as internal auditor's reports, the auditor considers whether the information provides a reliable basis and is sufficiently detailed for the auditor's purpose.

### Assessing the Risks of Material Misstatement

**100. The auditor should identify and assess the risks of material misstatement at the financial statement level, and at the assertion level for classes of transactions, account balances, and disclosures.** For this purpose, the auditor:

- Identifies risks throughout the process of obtaining an understanding of the entity and its environment, including relevant controls that relate to the risks, and by considering the classes of transactions, account balances, and disclosures in the financial statements;
- Relates the identified risks to what can go wrong at the assertion level;
- Considers whether the risks are of a magnitude that could result in a material misstatement of the financial statements; and
- Considers the likelihood that the risks could result in a material misstatement of the financial statements.

101. The auditor uses information gathered by performing risk assessment procedures, including the audit evidence obtained in evaluating the design of controls and determining whether they have been implemented, as audit evidence to support the risk assessment. The auditor uses the risk assessment to determine the nature, timing, and extent of further audit procedures to be performed.

102. The auditor determines whether the identified risks of material misstatement relate to specific classes of transactions, account balances, and disclosures and related assertions, or whether they relate more perva-

## FOR YOUR INFORMATION

sively to the financial statements as a whole and potentially affect many assertions. The latter risks (risks at the financial statement level) may increase particularly in case of a weak control environment.

103. The nature of the risks arising from a weak control environment is such that they are not likely to be confined to specific individual risks of material misstatement in particular classes of transactions, account balances, and disclosures. Rather, weaknesses such as management's lack of competence may have a more pervasive effect on the financial statements and may require an overall response by the auditor.
104. In making risk assessments, the auditor may identify the controls that are likely to prevent, or detect and correct, material misstatement in specific assertions. Generally, the auditor gains an understanding of controls and relates them to assertions in the context of processes and systems in which they exist. Doing so is useful because individual control activities often do not in themselves address a risk. Often only multiple control activities, together with other elements of internal control, will be sufficient to address a risk.
105. Conversely, some control activities may have a specific effect on an individual assertion embodied in a particular class of transactions or account balance. For example, the control activities that an entity established to ensure that its personnel are properly counting and recording the annual physical inventory relate directly to the existence and completeness assertions for the inventory account balance.
106. Controls can be either directly or indirectly related to an assertion. The more indirect the relationship, the less effective that control may be in preventing, or detecting and correcting, misstatements in that assertion. For example, a sales manager's review of a summary of sales activity for specific stores by region ordinarily is only indirectly related to the completeness assertion for sales revenue. Accordingly, it may be less effective in reducing risk for that assertion than controls more directly related to that assertion, such as matching shipping documents with billing documents.
107. The auditor's understanding of internal control may raise doubts about the auditability of an entity's financial statements. Concerns about the integrity of the entity's management may be so serious as to cause the auditor to conclude that the risk of management misrepresentation in the financial statements is such that an audit cannot be conducted. Also, concerns about the condition and reliability of an entity's records may cause the auditor to conclude that it is unlikely that sufficient appropriate audit evidence will be available to support an unqualified opinion on the financial statements. In such circumstances, the auditor considers a qualification or disclaimer of opinion, but in some

cases the auditor's only recourse may be to withdraw from the engagement.

### Significant Risks that Require Special Audit Consideration

**108. As part of the risk assessment as described in paragraph 100, the auditor should determine which of the risks identified are, in the auditor's judgment, risks that require special audit consideration (such risks are defined as "significant risks").**

109. The determination of significant risks, which arise on most audits, is a matter for the auditor's professional judgment. In exercising this judgment, the auditor excludes the effect of identified controls related to the risk to determine whether the nature of the risk, the likely magnitude of the potential misstatement including the possibility that the risk may give rise to multiple misstatements, and the likelihood of the risk occurring are such that they require special audit consideration. Routine, non-complex transactions that are subject to systematic processing are less likely to give rise to significant risks because they have lower inherent risks. On the other hand, significant risks are often derived from business risks that may result in a material misstatement. In considering the nature of the risks, the auditor considers a number of matters, including the following:
- Whether the risk is a risk of fraud.
  - Whether the risk is related to recent significant economic, accounting or other developments and, therefore, requires specific attention.
  - The complexity of transactions.
  - Whether the risk involves significant transactions with related parties.
  - The degree of subjectivity in the measurement of financial information related to the risk especially those involving a wide range of measurement uncertainty.
  - Whether the risk involves significant transactions that are outside the normal course of business for the entity, or that otherwise appear to be unusual.
110. Significant risks often relate to significant non-routine transactions and judgmental matters. Non-routine transactions are transactions that are unusual, either due to size or nature, and that therefore occur infrequently. Judgmental matters may include the development of accounting estimates for which there is significant measurement uncertainty.
111. Risks of material misstatement may be greater for risks relating to significant non-routine transactions arising from matters such as the following:
- Greater management intervention to specify the accounting treatment.
  - Greater manual intervention for data collection and processing.
  - Complex calculations or accounting principles.

## FOR YOUR INFORMATION

- The nature of non-routine transactions, which may make it difficult for the entity to implement effective controls over the risks.

112. Risks of material misstatement may be greater for risks relating to significant judgmental matters that require the development of accounting estimates, arising from matters such as the following:

- Accounting principles for accounting estimates or revenue recognition may be subject to differing interpretation.
- Required judgment may be subjective, complex or require assumptions about the effects of future events, for example, judgment about fair value.

**113. For significant risks, to the extent the auditor has not already done so, the auditor should evaluate the design of the entity's related controls, including relevant control activities, and determine whether they have been implemented.** An understanding of the entity's controls related to significant risks is required to provide the auditor with adequate information to develop an effective audit approach. Management ought to be aware of significant risks; however, risks relating to significant non-routine or judgmental matters are often less likely to be subject to routine controls. Therefore, the auditor's understanding of whether the entity has designed and implemented controls for such significant risks includes whether and how management responds to the risks and whether control activities such as a review of assumptions by senior management or experts, formal processes for estimations or approval by those charged with governance have been implemented to address the risks. For example, where there are one-off events such as the receipt of notice of a significant lawsuit, consideration of the entity's response will include such matters as whether it has been referred to appropriate experts (such as internal or external legal counsel), whether an assessment has been made of the potential effect, and how it is proposed that the circumstances are to be disclosed in the financial statements.

114. If management has not appropriately responded by implementing controls over significant risks and if, as a result, the auditor judges that there is a material weakness in the entity's internal control, the auditor communicates this matter to those charged with governance as required by paragraph 120. In these circumstances, the auditor also considers the implications for the auditor's risk assessment.

### Risks for which Substantive Procedures Alone Do Not Provide Sufficient Appropriate Audit Evidence

**115. As part of the risk assessment as described in paragraph 100, the auditor should evaluate the design and determine the implementation of the entity's controls, including relevant control activities, over**

**those risks for which, in the auditor's judgment, it is not possible or practicable to reduce the risks of material misstatement at the assertion level to an acceptably low level with audit evidence obtained only from substantive procedures.**

116. The understanding of the entity's information system relevant to financial reporting enables the auditor to identify risks of material misstatement that relate directly to the recording of routine classes of transactions or account balances, and the preparation of reliable financial statements; these include risks of inaccurate or incomplete processing. Ordinarily, such risks relate to significant classes of transactions such as an entity's revenue, purchases, and cash receipts or cash payments.

117. The characteristics of routine day-to-day business transactions often permit highly automated processing with little or no manual intervention. In such circumstances, it may not be possible to perform only substantive procedures in relation to the risk. For example, in circumstances where a significant amount of an entity's information is initiated, recorded, processed, or reported electronically such as in an integrated system, the auditor may determine that it is not possible to design effective substantive procedures that by themselves would provide sufficient appropriate audit evidence that relevant classes of transactions or account balances, are not materially misstated. In such cases, audit evidence may be available only in electronic form, and its sufficiency and appropriateness usually depend on the effectiveness of controls over its accuracy and completeness. Furthermore, the potential for improper initiation or alteration of information to occur and not be detected may be greater if information is initiated, recorded, processed or reported only in electronic form and appropriate controls are not operating effectively.

118. Examples of situations where the auditor may find it impossible to design effective substantive procedures that by themselves provide sufficient appropriate audit evidence that certain assertions are not materially misstated include the following:

- An entity that conducts its business using IT to initiate orders for the purchase and delivery of goods based on predetermined rules of what to order and in what quantities and to pay the related accounts payable based on system-generated decisions initiated upon the confirmed receipt of goods and terms of payment. No other documentation of orders placed or goods received is produced or maintained, other than through the IT system.
- An entity that provides services to customers via electronic media (for example, an Internet service provider or a telecommunications company) and uses IT to create a log of the services provided to its customers, initiate and process its billings for the services and automatically record such amounts in elec-

## FOR YOUR INFORMATION

tronic accounting records that are part of the system used to produce the entity's financial statements.

### Revision of Risk Assessment

119. The auditor's assessment of the risks of material misstatement at the assertion level is based on available audit evidence and may change during the course of the audit as additional audit evidence is obtained. In particular, the risk assessment may be based on an expectation that controls are operating effectively to prevent, or detect and correct, a material misstatement at the assertion level. In performing tests of controls to obtain audit evidence about their operating effectiveness, the auditor may obtain audit evidence that controls are not operating effectively at relevant times during the audit. Similarly, in performing substantive procedures the auditor may detect misstatements in amounts or frequency greater than is consistent with the auditor's risk assessments. In circumstances where the auditor obtains audit evidence from performing further audit procedures that tends to contradict the audit evidence on which the auditor originally based the assessment, the auditor revises the assessment and modifies the further planned audit procedures accordingly.

### Communicating With Those Charged With Governance and Management

**120. The auditor should make those charged with governance or management aware, as soon as practicable, and at an appropriate level of responsibility, of material weaknesses in the design or implementation of internal control which have come to the auditor's attention.**

121. If the auditor identifies risks of material misstatement which the entity has either not controlled, or for which the relevant control is inadequate, or if in the auditor's judgment there is a material weakness in the entity's risk assessment process, then the auditor includes such internal control weaknesses in the communication of audit matters of governance interest. See AAS 27 "Communications of Audit Matters With Those Charged With Governance."

### Documentation

**122. The auditor should document:**

- (a) **The discussion among the engagement team regarding the susceptibility of the entity's financial statements to material misstatement due to error or fraud, and the significant decisions reached;**
- (b) **Key elements of the understanding obtained regarding each of the aspects of the entity and its environment identified in paragraph 20, including each of the internal control components**

**identified in paragraph 43, to assess the risks of material misstatement of the financial statements; the sources of information from which the understanding was obtained; and the risk assessment procedures;**

- (c) **The identified and assessed risks of material misstatement at the financial statement level and at the assertion level as required by paragraph 100; and**
- (d) **The risks identified and related controls evaluated as a result of the requirements in paragraphs 113 and 115.**

123. The manner in which these matters are documented is for the auditor to determine using professional judgment. In particular, the results of the risk assessment may be documented separately, or may be documented as part of the auditor's documentation of further procedures. Examples of common techniques, used alone or in combination include narrative descriptions, questionnaires, check lists and flow charts. Such techniques may also be useful in documenting the auditor's assessment of the risks of material misstatement at the overall financial statement and assertions level. The form and extent of this documentation is influenced by the nature, size and complexity of the entity and its internal control, availability of information from the entity and the specific audit methodology and technology used in the course of the audit. For example, documentation of the understanding of a complex information system in which a large volume of transactions are electronically initiated, recorded, processed, or reported may include flowcharts, questionnaires, or decision tables. For an information system making limited or no use of IT or for which few transactions are processed (say, long-term debt), documentation in the form of a memorandum may be sufficient. Ordinarily, the more complex the entity and the more extensive the audit procedures performed by the auditor, the more extensive the auditor's documentation will be. AAS 3, "Documentation" provides guidance regarding documentation in the context of the audit of financial statements.

### Effective Date

124. This Auditing and Assurance Standards is effective for audits related to accounting periods beginning on or after 1st April, 2007.

### Compatibility with the International Standard on Auditing (ISA) 315

The auditing standards established in this AAS are generally consistent in all material respects with those set out in ISA 315, "Understanding The Entity And Its Environment And Assessing The Risks Of Material Misstatement".

## Appendix 1: Understanding the Entity and Its Environment

(Refer paragraph 20)

This appendix provides additional guidance on matters the auditor may consider when obtaining an understanding of the industry, regulatory, and other external factors that affect the entity, including the applicable financial reporting framework; the nature of the entity; objectives and strategies and related business risks; and measurement and review of the entity's financial performance. The examples provided cover a broad range of matters applicable to many engagements; however, not all matters are relevant to every engagement and the list of examples is not necessarily complete. Additional guidance on internal control is contained in **Appendix 2**.

### Industry, Regulatory and Other External Factors, Including The Applicable Financial Reporting Framework

Examples of matters an auditor may consider include the following:

- Industry conditions
  - The market and competition, including demand, capacity, and price competition
  - Cyclical or seasonal activity
  - Product technology relating to the entity's products
  - Energy supply and cost
- Regulatory environment
  - Accounting principles and industry specific practices
  - Regulatory framework for a regulated industry
  - Legislation and regulation that significantly affect the entity's operations
    - Regulatory requirements
    - Direct supervisory activities
  - Taxation (corporate and other)
  - Government policies currently affecting the conduct of the entity's business
    - Monetary, including foreign exchange controls
    - Fiscal
    - Financial incentives (for example, government aid programs)
    - Tariffs, trade restrictions
  - Environmental requirements affecting the industry and the entity's business
- Other external factors currently affecting the entity's business
  - General level of economic activity (for example, recession, growth)
  - Interest rates and availability of financing
  - Inflation, currency revaluation

### Nature of the Entity

Examples of matters an auditor may consider include the following:

#### *Management and ownership*

- Structure of the entity (corporate and non corporate)
  - private, public, government (including any recent

- or planned changes)
- Organizational structure
- Board of directors – corporate form
  - Composition
  - Business reputation and experience of individuals
  - Independence from and control over operating management
  - Frequency of meetings
  - Existence of audit committee and scope of its activities
  - Existence of policy on corporate conduct
- Members of managing committee (by whatever name called)
  - Composition and election of members
  - Business reputation and experience of individuals
  - Independence from and control over operating management
  - Frequency of meetings
  - Existence of audit committee and scope of its activities
  - Existence of policy on conduct of business by the enterprise
- Operating management
  - Experience and reputation
  - Turnover
  - Key financial personnel and their status in the organisation
  - Staffing of accounting department
  - Incentives or bonus plans as part of remuneration
  - Use of forecasts and budgets
  - Pressures on management (for example, over extended dominance by one individual, unreasonable deadlines for announcing results)
  - Management information systems
- Internal audit function – existence and quality
- Attitude to internal control environment

### Business Operations

Nature of revenue sources (for example, manufacturer, wholesaler, banking, insurance or other financial services, import/export trading, utility, transportation, and technology products and services)

- Products or services and markets (for example, major customers and contracts, terms of payment, profit margins, market share, competitors, exports, pricing policies, reputation of products, warranties, order book, trends, marketing strategy and objectives, manufacturing processes)
- Conduct of operations (for example, stages and methods of production, business segments, delivery or products and services, details of declining or expanding operations)
- Alliances, joint ventures, and outsourcing activities

## FOR YOUR INFORMATION

- Involvement in electronic commerce, including Internet sales and marketing activities
- Geographic dispersion and industry segmentation
- Location of production facilities, warehouses, and offices
- Key customers
- Important suppliers of goods and services (for example, long-term contracts, stability of supply, terms of payment, imports, methods of delivery such as “just-in-time”)
- Employment (for example, by location, supply, wage levels, union contracts, pension and other post employment benefits, stock option or incentive bonus arrangements, and government regulation related to employment matters)
- Research and development activities and expenditures
- Transactions with related parties

### Investments

- Acquisitions, mergers or disposals of business activities (planned or recently executed)
- Investments and dispositions of securities and loans
- Capital investment activities, including investments in plant and equipment and technology, and any recent or planned changes
- Investments in non-consolidated entities, including partnerships, joint ventures and special-purpose entities

### Financing

- Capital structure (including any recent or planned changes)
- Group structure – major subsidiaries and associated entities, including consolidated and non-consolidated structures
- Debt structure, including covenants, restrictions, guarantees, and off-balance-sheet financing arrangements
- Leasing of property, plant or equipment for use in the business
- Beneficial owners (local, foreign, business reputation and experience)
- Beneficial owners and related parties (local, foreign, business reputation and experience)
- Use of derivative financial instruments
- Business restructuring – acquisitions, mergers or disposals of business activities (planned or recently executed)

### Financial Reporting

- Accounting principles and industry specific practices
- Revenue recognition practices
- Accounting for fair values
- Inventories (for example, locations, quantities)
- Foreign currency assets, liabilities and transactions
- Industry-specific significant categories (for example, loans and investments for banks, accounts receivable and inventory for manufacturers, research and development for pharmaceuticals)
- Accounting for unusual or complex transactions

including those in controversial or emerging areas (for example, accounting for stock-based compensation)

- Financial statement presentation and disclosure

### Objectives and Strategies and Related Business Risks.

Examples of matters an auditor may consider include the following:

- Management philosophy, strategic plans
- Existence of objectives (i.e., how the entity addresses industry, regulatory and other external factors) relating to, for example, the following:
  - Industry developments (a potential related business risk might be, for example, that the entity does not have the personnel or expertise to deal with the changes in the industry)
  - New products and services (a potential related business risk might be, for example, that there is increased product liability)
  - Expansion of the business (a potential related business risk might be, for example, that the demand has not been accurately estimated)
  - New accounting requirements (a potential related business risk might be, for example, incomplete or improper implementation, or increased costs)
  - Regulatory requirements (a potential related business risk might be, for example, that there is increased legal exposure)
  - Current and prospective financing requirements (a potential related business risk might be, for example, the loss of financing due to the entity’s inability to meet requirements)
  - Use of IT (a potential related business risk might be, for example, that systems and processes are incompatible)
- Effects of implementing a strategy, particularly any effects that will lead to new accounting requirements (a potential related business risk might be, for example, incomplete or improper implementation)

### Measurement and Review of the Entity’s Financial Performance

- Examples of matters an auditor may consider include the following:
  - Key ratios and operating statistics
  - Key performance indicators
  - Employee performance measures and incentive compensation policies
  - Trends
  - Use of forecasts, budgets and variance analysis
  - Analyst reports and credit rating reports
  - Competitor analysis
  - Period-on-period financial performance (revenue growth, profitability, leverage)

## Appendix 2: Internal Control Components

*(Refer paragraphs 20, 43 and 58)*

1. As set out in paragraph 43 and described in paragraphs 67-99, internal control consists of the following components:
  - (a) The control environment;
  - (b) The entity's risk assessment process;
  - (c) The information system, including the related business processes, relevant to financial reporting, and communication;
  - (d) Control activities; and
  - (e) Monitoring of controls.

This appendix further explains the above components as they relate to a financial statement audit.

### Control Environment

2. The control environment includes the attitudes, awareness, and actions of management and those charged with governance concerning the entity's internal control and its importance in the entity. The control environment also includes the governance and management functions and sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for effective internal control, providing discipline and structure.
3. The control environment encompasses the following elements:
  - (a) *Communication and enforcement of integrity and ethical values* - The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment which influence the effectiveness of the design, administration, and monitoring of other components of internal control. Integrity and ethical behaviour are the product of the entity's ethical and behavioural standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioural standards to personnel through policy statements and codes of conduct and by example.
  - (b) *Commitment to competence* - Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.
  - (c) *Participation by those charged with governance* - An entity's control consciousness is influenced sig-

nificantly by those charged with governance. Attributes of those charged with governance include independence from management, their experience and stature, the extent of their involvement and scrutiny of activities, the appropriateness of their actions, the information they receive, the degree to which difficult questions are raised and pursued with management, and their interaction with internal and external auditors. The importance of responsibilities of those charged with governance is recognized in codes of practice and other regulations or guidance produced for the benefit of those charged with governance. Other responsibilities of those charged with governance include oversight of the design and effective operation of whistle blower procedures and the process for reviewing the effectiveness of the entity's internal control.

- (d) *Management's philosophy and operating style* - Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risks; management's attitudes and actions toward financial reporting (conservative or aggressive selection from available alternative accounting principles, and conscientiousness and conservatism with which accounting estimates are developed); and management's attitudes toward information processing and accounting functions and personnel.
- (e) *Organizational structure* - An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and reviewed. Establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. An entity develops an organizational structure suited to its needs. The appropriateness of an entity's organizational structure depends, in part, on its size and the nature of its activities.
- (f) *Assignment of authority and responsibility* - This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize

how and for what they will be held accountable.

- (g) *Human resource policies and practices* - Human resource policies and practices relate to recruitment, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. For example, standards for recruiting the most qualified individuals – with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behaviour – demonstrate an entity’s commitment to competent and trustworthy people. Training policies that communicate prospective roles and responsibilities and include practices such as training schools and seminars illustrate expected levels of performance and behaviour. Promotions driven by periodic performance appraisals demonstrate the entity’s commitment to the advancement of qualified personnel to higher levels of responsibility.

### *Application to Small Entities*

4. Small entities may implement the control environment elements differently than larger entities. For example, small entities might not have a written code of conduct but, instead, develop a culture that emphasizes the importance of integrity and ethical behaviour through oral communication and by management example. Similarly, those charged with governance in small entities may not include an independent or outside member.

### **Entity’s Risk Assessment Process**

5. An entity’s risk assessment process is its process for identifying and responding to business risks and the results thereof. For financial reporting purposes, the entity’s risk assessment process includes how management:
  - identifies risks relevant to the preparation of financial statements that give a true and fair view (or are presented fairly, in all material respects)<sup>3</sup>;
  - estimates their significance;
  - assesses the likelihood of their occurrence; and
  - decides upon actions to manage them.

For example, the entity’s risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting also relate to specific events or transactions.

6. Risks relevant to financial reporting include external and internal events and circumstances that may occur and adversely affect an entity’s ability to initiate,

record, process, and report financial data consistent with the assertions of management in the financial statements. Once risks are identified, management considers their significance, the likelihood of their occurrence, and how they should be managed. Management may initiate plans, programs, or actions to address specific risks or it may decide to accept a risk because of cost or other considerations. Risks can arise or change due to circumstances such as the following:

- Changes in operating environment. Changes in the regulatory or operating environment can result in changes in competitive pressures and significantly different risks.
- New personnel. New personnel may have a different focus on or understanding of internal control.
- New or revamped information systems. Significant and rapid changes in information systems can change the risk relating to internal control.
- Rapid growth. Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.
- New technology. Incorporating new technologies into production processes or information systems may change the risk associated with internal control.
- New business models, products, or activities. Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with internal control.
- Corporate restructurings. Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with internal control.
- Expanded foreign operations. The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.
- New accounting pronouncements. Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.

### *Application to Small Entities*

7. The basic concepts of the entity’s risk assessment process are relevant to every entity, regardless of size, but the risk assessment process is likely to be less formal and less structured in small entities than in larger ones. All entities should have established financial reporting objectives, but they may be recognized implicitly rather than explicitly in small entities.

<sup>3</sup> In accordance with the financial reporting framework applicable to the entity.

## FOR YOUR INFORMATION

Management may be aware of risks related to these objectives without the use of a formal process but through direct personal involvement with employees and outside parties.

### Information System, Including the Related Business Processes, Relevant to Financial Reporting, and Communication

8. An information system consists of infrastructure (physical and hardware components), software, people, procedures, and data. Infrastructure and software will be absent, or have less significance, in systems that are exclusively or primarily manual. Many information systems make extensive use of information technology (IT).
9. The information system relevant to financial reporting objectives, which includes the financial reporting system, consists of the procedures and records established to initiate, record, process, and report entity transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity. Transactions may be initiated manually or automatically by programmed procedures. Recording includes identifying and capturing the relevant information for transactions or events. Processing includes functions such as edit and validation, calculation, measurement, valuation, summarization, and reconciliation, whether performed by automated or manual procedures. Reporting relates to the preparation of financial reports as well as other information, in electronic or printed format, that the entity uses in measuring and reviewing the entity's financial performance and in other functions. The quality of system-generated information affects management's ability to make appropriate decisions in managing and controlling the entity's activities and to prepare reliable financial reports.
10. Accordingly, an information system encompasses methods and records that:
  - Identify and record all valid transactions.
  - Describe on a timely basis the transactions in sufficient detail to permit proper classification of transactions for financial reporting.
  - Measure the value of transactions in a manner that permits recording their proper monetary value in the financial statements.
  - Determine the time period in which transactions occurred to permit recording of transactions in the proper accounting period.
  - Present properly the transactions and related disclosures in the financial statements.
11. Communication involves providing an understanding of individual roles and responsibilities pertaining to

internal control over financial reporting. It includes the extent to which personnel understand how their activities in the financial reporting information system relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity. Open communication channels help ensure that exceptions are reported and acted on.

12. Communication takes such forms as policy manuals, accounting and financial reporting manuals, and memoranda. Communication also can be made electronically, orally, and through the actions of management.

### Application to Small Entities

13. Information systems and related business processes relevant to financial reporting in small entities are likely to be less formal than in larger entities, but their role is just as significant. Small entities with active management involvement may not need extensive descriptions of accounting procedures, sophisticated accounting records, or written policies. Communication may be less formal and easier to achieve in a small entity than in a larger entity due to the small entity's size and fewer levels as well as management's greater visibility and availability.

### Control Activities

14. Control activities are the policies and procedures that help ensure that management directives are carried out, for example, that necessary actions are taken to address risks that threaten the achievement of the entity's objectives. Control activities, whether within IT or manual systems, have various objectives and are applied at various organizational and functional levels.
15. Generally, control activities that may be relevant to an audit may be categorized as policies and procedures that pertain to the following:
  - *Performance reviews* - These control activities include reviews and analysis of actual performance versus budgets, forecasts, and prior period performance; relating different sets of data – operating or financial – to one another, together with analysis of the relationships and investigative and corrective actions; comparing internal data with external sources of information; and review of functional or activity performance, such as a bank's consumer loan manager's review of reports by branch, region, and loan type for loan approvals and collections.
  - *Information processing* - A variety of controls are performed to check accuracy, completeness, and authorization of transactions. The two broad groupings of information systems control activities are application controls and general IT-controls. Application controls apply to the processing of indi-

vidual applications. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. Examples of application controls include checking the arithmetical accuracy of records, maintaining and reviewing accounts and trial balances, automated controls such as edit checks of input data and numerical sequence checks, and manual follow-up of exception reports. General IT-controls are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. General IT-controls commonly include controls over data centre and network operations; system software acquisition, change and maintenance; access security; and application system acquisition, development, and maintenance. These controls apply to mainframe, miniframe, and end-user environments. Examples of such general IT-controls are program change controls, controls that restrict access to programs or data, controls over the implementation of new releases of packaged software applications, and controls over system software that restrict access to or monitor the use of system utilities that could change financial data or records without leaving an audit trail.

- *Physical controls* - These activities encompass the physical security of assets, including adequate safeguards such as secured facilities over access to assets and records; authorization for access to computer programs and data files; and periodic counting and comparison with amounts shown on control records (for example comparing the results of cash, security and inventory counts with accounting records). The extent to which physical controls intended to prevent theft of assets are relevant to the reliability of financial statement preparation, and therefore the audit, depends on circumstances such as when assets are highly susceptible to misappropriation. For example, these controls would ordinarily not be relevant when any inventory losses would be detected pursuant to periodic physical inspection and recorded in the financial statements. However, if for financial reporting purposes management relies solely on perpetual inventory records, the physical security controls would be relevant to the audit.
- *Segregation of duties* - Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the person's duties. Examples of segregation of duties include reporting, reviewing and approving recon-

ciliations, and approval and control of documents.

16. Certain control activities may depend on the existence of appropriate higher level policies established by management or those charged with governance. For example, authorization controls may be delegated under established guidelines, such as investment criteria set by those charged with governance; alternatively, non-routine transactions such as major acquisitions or divestments may require specific high level approval, including in some cases that of shareholders.

### *Application to Small Entities*

17. The concepts underlying control activities in small entities are likely to be similar to those in larger entities, but the formality with which they operate varies. Further, small entities may find that certain types of control activities are not relevant because of controls applied by management. For example, management's retention of authority for approving credit sales, significant purchases, and draw-downs on lines of credit can provide strong control over those activities, lessening or removing the need for more detailed control activities. An appropriate segregation of duties often appears to present difficulties in small entities. Even companies that have only a few employees, however, may be able to assign their responsibilities to achieve appropriate segregation or, if that is not possible, to use management oversight of the incompatible activities to achieve control objectives.

### **Monitoring of Controls**

18. An important management responsibility is to establish and maintain internal control on an ongoing basis. Management's monitoring of controls includes considering whether they are operating as intended and that they are modified as appropriate for changes in conditions. Monitoring of controls may include activities such as management's review of whether bank reconciliations are being prepared on a timely basis, internal auditors evaluation of sales personnel's compliance with the entity's policies on terms of sales contracts, and a legal department's oversight of compliance with the entity's ethical or business practice policies.
19. Monitoring of controls is a process to assess the quality of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions. Monitoring is done to ensure that controls continue to operate effectively. For example, if the timeliness and accuracy of bank reconciliations are not monitored, personnel are likely to stop preparing them. Monitoring of controls is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.
20. Ongoing monitoring activities are built into the normal recurring activities of an entity and include regular management and supervisory activities. Managers of

## FOR YOUR INFORMATION

sales, purchasing, and production at divisional and corporate levels are in touch with operations and may question reports that differ significantly from their knowledge of operations.

21. In many entities, internal auditors or personnel performing similar functions contribute to the monitoring of an entity's controls through separate evaluations. They regularly provide information about the functioning of internal control, focusing considerable attention on evaluating the design and operation of internal control. They communicate information about strengths and weaknesses and recommendations for improving internal control.
22. Monitoring activities may include using information from communications from external parties that may indicate problems or highlight areas in need of improvement. Customers implicitly corroborate

billing data by paying their invoices or complaining about their charges. In addition, regulators may communicate with the entity concerning matters that affect the functioning of internal control, for example, communications concerning examinations by bank regulatory agencies. Also, management may consider communications relating to internal control from external auditors in performing monitoring activities.

### *Application to Small Entities*

23. Ongoing monitoring activities of small entities are more likely to be informal and are typically performed as a part of the overall management of the entity's operations. Management's close involvement in operations often will identify significant variances from expectations and inaccuracies in financial data leading to corrective action to the control.

### **Appendix 3: Conditions and Events that May Indicate Risks of Material Misstatement**

*(Refer paragraph 32)*

The following are examples of conditions and events that may indicate the existence of risks of material misstatement. The examples provided cover a broad range of conditions and events; however, not all conditions and events are relevant to every audit engagement and the list of examples is not necessarily complete.

- Operations in regions that are economically unstable, for example, countries with significant currency devaluation or highly inflationary economies.
- Operations exposed to volatile markets, for example, futures trading.
- High degree of complex regulation.
- Going concern and liquidity issues including loss of significant customers.
- Constraints on the availability of capital and credit.
- Changes in the industry in which the entity operates.
- Changes in the supply chain.
- Developing or offering new products or services, or moving into new lines of business.
- Expanding into new locations.
- Changes in the entity such as large acquisitions or reorganizations or other unusual events.
- Entities or business segments likely to be sold.
- Complex alliances and joint ventures.
- Use of off-balance-sheet finance, special-purpose entities, and other complex financing arrangements.
- Significant transactions with related parties.
- Lack of personnel with appropriate accounting and financial reporting skills.
- Changes in key personnel including departure of key executives.
- Weaknesses in internal control, especially those not addressed by management.
- Inconsistencies between the entity's IT strategy and its business strategies.
- Changes in the IT environment.
- Installation of significant new IT systems related to financial reporting.
- Inquiries into the entity's operations or financial results by regulatory or government bodies.
- Past misstatements, history of errors or a significant amount of adjustments at period end.
- Significant amount of non-routine or non-systematic transactions including intercompany transactions and large revenue transactions at period end.
- Transactions that are recorded based on management's intent, for example, debt refinancing, assets to be sold and classification of marketable securities.
- Application of new accounting pronouncements.
- Accounting measurements that involve complex processes.
- Events or transactions that involve significant measurement uncertainty, including accounting estimates.
- Pending litigation and contingent liabilities, for example, sales warranties, financial guarantees and environmental remediation.