

INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS 3402

Assurance Reports on a Service Organization's Controls

Introduction

Scope of this ISA

1. This International Standard on Assurance Engagements (ISAE) deals with assurance engagements to report on the controls of an organization that provides a service to user entities when the service organization considers those controls are likely to be part of user entities' information systems, including the related business processes, relevant to financial reporting. It complements [proposed] ISA 402 (Revised and Redrafted), "Audit Considerations Relating to an Entity Using a Third Party Service Organization," in that reports prepared in accordance with this ISAE are capable of providing appropriate evidence under [proposed] ISA 402 (Revised and Redrafted).
2. This ISAE may also be applied, adapted as necessary in the circumstances of the engagement, for engagements to report on other controls at third party organizations as they relate to user entities, e.g., controls that affect entities' regulatory compliance, production or quality control.
3. In addition to issuing an assurance report on controls, a service auditor may also be engaged to provide the following reports which are not dealt with in this ISAE:
 - (a) An audit report on a user entity's transactions or balances maintained by the service organization; or
 - (b) An agreed-upon procedures report on controls at a service organization, or on a user entity's transactions or balances maintained by the service organization.
4. The "International Framework for Assurance Engagements" (the Assurance Framework) notes that an assurance engagement may be either an "assertion-based" engagement or a "direct reporting" engagement. This ISAE is written in terms of an assertion-based engagement.

Relationship with other professional pronouncements

5. When preparing an assurance report on a service organization's controls that are part of user entities' information systems relevant to financial reporting, the service auditor is required by paragraph 11 of this ISAE to comply with ISAE 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information," in addition to this ISAE. The Assurance Framework, which defines and describes the elements and objectives of an assurance engagement, provides the context for understanding this ISAE and ISAE 3000.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

6. Compliance with ISAE 3000 requires, amongst other things, that the service auditor comply with the Code of Ethics for Professional Accountants (the Code), and implement quality control procedures that are applicable to the individual engagement.

<i>See Issues Paper – Issue I “Link with ISAE 3000 and the ISAs – Quality Control”</i>
--

Effective Date

8. This ISAE is effective for service auditor’s reports dated on or after [date].

Objectives

9. The objectives of the service auditor are to:
 - (a) Obtain reasonable assurance about whether, in all material respects:
 - (i) Management’s description of the system, control objectives and related controls is fairly presented;
 - (ii) The controls are suitably designed to provide reasonable assurance that the specified control objectives will be achieved if the controls operate effectively;
 - (iii) When included in the scope of the engagement, the controls operated effectively; and
 - (b) Report in accordance with the service auditor’s findings.

Definitions

10. For purposes of this ISAE, the following terms have the meanings attributed below:
 - (a) User Entity – An entity that uses a service organization that performs services that are part of the entity’s information system relevant to financial reporting.
 - (b) User Auditor – An auditor who audits and reports on the financial statements of a user entity.
 - (c) Service Organization – An organization (or segment of an organization) that provides services to user entities that are part of the entity’s information system relevant to financial reporting.
 - (d) Service Auditor – An auditor who provides an assurance report on the controls of a service organization.
 - (e) Service Organization’s Controls – The process designed, implemented and maintained by the service organization to provide reasonable assurance about the achievement of the control objectives that are relevant to services covered by the service auditor’s report. (Ref: Para. A1)
 - (f) Control Objectives – The aim or purpose of a particular aspect of the service organization’s controls. Control objectives ordinarily relate to risks that controls seek to mitigate. Examples of control objectives are provided in Appendix 1.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- (g) Complementary User Entity Controls – Controls that must be implemented by user entities in order to achieve control objectives specified by a service organization.

<i>See Issues Paper – Issue H “Complementary controls”</i>
--

- (h) Report on the Description, Design and Operating Effectiveness of Controls at a Service Organization (referred to in this ISAE as a Type B report) – A report that comprises:
 - (i) A description of the system, control objectives and related controls prepared by management of the service organization;
 - (ii) A written assertion by the service organization’s management that, in all material respects, and based on suitable criteria:
 - (a) The description presents fairly relevant aspects of the system, control objectives and related controls that had been designed and implemented throughout a specified period;
 - (b) The controls related to the control objectives included in the description were suitably designed throughout the specified period; and
 - (c) The controls related to the control objectives included in the description operated effectively throughout the specified period;
 - (iii) A service auditor’s assurance report that:
 - (a) Conveys a reasonable level of assurance about the matters in (ii)(a)-(c) above; and
 - (b) Includes a description of the service auditor’s tests of the controls and the results thereof.
- (i) Report on the Description and Design of Controls at a Service Organization (referred to in this ISAE as a Type A report) – A report that comprises:
 - (i) A description of the system, control objectives and related controls prepared by management of the service organization;
 - (ii) A written assertion by the service organization’s management that, in all material respects, and based on suitable criteria:
 - (a) The description presents fairly relevant aspects of the system, control objectives and related controls that had been designed and implemented as at a specified date;
 - (b) The controls related to the control objectives included in the description were suitably designed as at the specified date; and
 - (iii) A service auditor’s assurance report that conveys a reasonable level of assurance about the matters in (ii)(a) and (b) above.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

See Issues Paper – Issue F “Type A Reports”

- (j) Subservice Organization – A service organization used by another service organization to perform some or all of the services provided to a user entity that are part of a user entity’s information system relevant to financial reporting.
- (k) Subservice Organization’s Controls – The process designed, implemented and maintained by the subservice organization to provide reasonable assurance about the achievement of the control objectives that are relevant to the services covered by the service auditor’s report.
- (l) The Inclusive Method – Method of dealing with the services provided by a subservice organization, whereby the subservice organization’s relevant control objectives and related controls are included in the service organization’s description of the system, control objectives and related controls, and in the scope of the service auditor’s engagement.
- (m) The Carve-out Method – Method of dealing with the services provided by a subservice organization, whereby the subservice organization’s relevant control objectives and related controls are excluded from the service organization’s description of the system, control objectives and related controls, and from the scope of the service auditor’s engagement. The service organization’s description of the system, control objectives and related controls, and the scope of the service auditor’s engagement do, however, include controls at the service organization to monitor the effectiveness of controls at the subservice organization, which may include the service organization’s review of a Type B or Type A report on controls at the subservice organization.
- (n) Test of Controls – A procedure designed to evaluate the operating effectiveness of controls in preventing, or detecting and correcting, errors that could result in the non-achievement of specified control objectives.
- (o) Relevant Controls – Those service organization’s controls that are necessary to achieve the control objectives specified in the description of the system, control objectives and related controls.
- (p) Criteria – Benchmarks used to evaluate or measure the subject matter including, where relevant, benchmarks for presentation and disclosure. Suitable criteria are required for reasonably consistent evaluation or measurement of a subject matter within the context of professional judgment. Criteria need to be available to the intended users to allow them to understand how the subject matter has been evaluated or measured.

Requirements

ISAE 3000

11. In addition to this ISAE, the service auditor shall comply with ISAE 3000.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

See Issues Paper – Issue I “Link with ISAE 3000 and the ISAs – Limitation to qualified accountants”

Ethical Requirements

12. As required by the Code, the service auditor shall be independent from the service organization. However, in performing an engagement in accordance with this ISAE, the Code does not require the service auditor to be independent from each user entity.

See Issues Paper – Issue D “Independence”

Acceptance and Continuance

13. The service auditor shall accept (or continue where applicable) an engagement only if:
- (a) On the basis of a preliminary knowledge of the engagement circumstances, nothing comes to the attention of the service auditor to indicate that:

See Issues Paper – Issue I “Link with ISAE 3000 and the ISAs – Engagement acceptance”

- (i) The criteria to be used will not be suitable and available to the intended users;
- (ii) The service auditor will not have access to sufficient appropriate evidence, including the engagement team being involved in the work of subservice organization auditors, if any, to the extent necessary; and
- (iii) The description of the system, control objectives and related controls included in the scope of the engagement will not be so limited that it is unlikely that the engagement has a rational purpose; (Ref: Para. A2)
- (b) In agreeing the terms of the engagement, the service organization acknowledges that it understands and accepts its responsibility for:
- (i) Preparing and presenting the description of the system, control objectives and related controls, and accompanying assertions, including the completeness, accuracy and method of presentation of the description and assertions;
- (ii) Providing the services covered by the description of the system, control objectives and related controls;
- (iii) Identifying the control objectives (where not identified by law or regulation, or another party, e.g., a user group), and the risks that threaten their achievement;
- (iv) Designing, implementing and maintaining controls to achieve the identified control objectives; and
- (v) Providing complete information to the service auditor in connection with the engagement.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Assessing the Suitability of the Criteria

14. As required by ISAE 3000, the service auditor shall assess whether suitable criteria have been used by the service organization in preparing and presenting the description of the system, control objectives and related controls, in asserting that controls are suitably designed, and, in the case of a Type B report, that controls are operating effectively.
15. In assessing the suitability of the criteria used by management to evaluate the fair presentation of the description of the system, control objectives and related controls, the auditor shall determine that the criteria cover that the description:

<i>See Issues Paper – Issue B “Criteria”</i>
--

- (a) Presents how the system made available to user entities has been designed and implemented to process relevant transactions, including, as appropriate:
 - (i) The classes of transactions processed;
 - (ii) The procedures, within both information technology and manual systems, by which transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities;
 - (iii) The related accounting records, supporting information and specific accounts that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities;
 - (iv) How the system captures significant events and conditions, other than transactions;
 - (v) The process used to prepare reports presented to user entities; and
 - (vi) Other aspects of the service organization’s control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to processing and reporting user entities’ transactions.
 - (b) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is presented to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.
16. In assessing the suitability of the criteria used by management to evaluate the design of controls, the auditor shall determine that the criteria cover that the controls provide reasonable assurance that the related control objectives would be achieved if the controls are operated as described.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

17. In assessing the suitability of the criteria used by management to evaluate the effective operation of controls, the auditor shall determine that the criteria cover that the controls operated as described so as to provide reasonable assurance that the related control objectives were achieved throughout the specified period. (Ref: Para. A3)

Using the Work of Others

See Issues Paper – Issue I “Link with ISAE 3000 and the ISAs – Using the Work of an Expert”

18. If the service auditor uses the work of the internal audit function,¹ another auditor (including a subservice auditor), or an external expert, the service auditor shall:
- (a) Evaluate the capabilities, competence and objectivity of that other party, and the adequacy of that work for the purposes of the assurance engagement; and
 - (b) Make no reference to that other party or that work in the section of the service auditor’s assurance report that contains the service auditor’s opinion. (Ref: Para. A4-A5)

Obtaining an Understanding of the System

19. The service auditor shall obtain an understanding of the relevant aspects of the system, including controls, provided by the service organization and included in the scope of the engagement. (Ref: Para. A6-A7)

Obtaining Evidence Regarding the Description

20. The service auditor shall obtain and read the service organization’s description of the system, control objectives and related controls covered by the engagement, and shall evaluate whether that description is materially misstated, including whether:
- (a) Specified control objectives are reasonable in the circumstances;
 - (b) Controls identified in the description were implemented; and
 - (c) Complementary user entity controls, if any, are adequately described.
21. The service auditor’s procedures shall include inquiries of management and other service organization personnel, and observation and inspection of records and other documentation of the manner in which transactions are processed through the system and controls are applied, to confirm the implementation of the controls. (Ref: Para. A8-A11)

Obtaining Evidence Regarding Design of Controls

22. The service auditor shall determine which of the service organization’s controls are relevant controls, and shall assess whether they were suitably designed. This shall include:

¹ As used in this ISAE, the term “internal audit function” also includes others (by whatever name, e.g., a compliance or risk department) who perform similar activities to internal audit functions (see A4).

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- (a) Identifying the risks that threaten the achievement of the specified control objectives; and
- (b) Evaluating the linkage of the relevant controls identified in the description with those risks. (Ref: Para. A12-A14)

Obtaining Evidence Regarding Effectiveness of Controls

23. If providing a Type B report, the service auditor shall assess the operating effectiveness of relevant controls. When testing a relevant control, the service auditor shall:
- (a) Perform other procedures in combination with inquiry to obtain evidence about:
 - (i) How the control was applied.
 - (ii) The consistency with which the control was applied.
 - (iii) By who or by what means the control was applied.
 - (b) Determine whether relevant controls to be tested depend upon other controls (indirect controls), and if so, whether it is necessary to obtain evidence supporting the operating effectiveness of those indirect controls; and
 - (c) Determine the extent of tests of controls taking account of factors that include the nature of relevant controls, the frequency of their application (e.g., monthly, daily, many times per day), and the expected rate of deviation.
24. When one or more deviations from a relevant control are detected, the service auditor shall evaluate the nature and number of the deviations and their potential consequences, and determine whether:
- (a) Identified deviations are within the expected rate of deviation and are acceptable; therefore, the testing that has been performed provides an appropriate basis for concluding that the control is operating effectively throughout the specified period;
 - (b) Additional testing of the control is necessary to reach a conclusion on whether the control is operating effectively throughout the specified period; or
 - (c) The testing that has been performed provides an appropriate basis for concluding that the control did not operate effectively throughout the specified period. (Ref: Para. A15-A21)

Written Representations

25. The service auditor shall request management to provide written representations whether all records, documentation, unusual matters of which management is aware, and other information relevant to the assurance engagement has been made available to the service auditor, and that management has disclosed to the service auditor any of the following of which management is aware:

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- (a) Illegal acts, fraud or uncorrected errors attributable to the service organization's management or employees that may affect one or more user entities;
 - (b) Design deficiencies in controls, including those for which management believes the cost of corrective action may exceed the benefits;
 - (c) Instances where controls have not operated as described; and
 - (d) Subsequent events that would have a significant effect on user entities.
- 26. The written representations noted in paragraph 25, shall be in the form of a representation letter addressed to the service auditor, and shall be as of the same date as the service auditor's assurance report.
- 27. If management does not provide the written representations requested by the service auditor in accordance with paragraph 25, the auditor shall:
 - (a) Ask for the reasons;
 - (b) Reconsider the assessment of the integrity of management; and
 - (c) Take appropriate actions, including determining the possible effects on the opinion in the service auditor's report. (Ref: Para. A22)

Illegal Acts, Fraud or Uncorrected Errors

- 28. If the service auditor becomes aware of illegal acts, fraud or uncorrected errors that have not been communicated appropriately to affected user entities, and management of the service organization is unwilling to do so, the service auditor shall take appropriate action. (Ref: Para. A23)

Other Information

- 29. The service auditor shall read the other information, if any, included in a document containing the description of the system, control objectives and related controls that is provided to user entities on the same terms and at the same time as the description of the system, control objectives and related controls, to identify material inconsistencies, if any, with that description. While reading the other information for the purpose of identifying material inconsistencies, the service auditor may become aware of an apparent misstatement of fact.
- 30. If the auditor becomes aware of a material inconsistency or an apparent misstatement of fact, the auditor shall discuss the matter with management. If the auditor concludes that there is a material inconsistency or a misstatement of fact that management refuses to correct, the auditor shall take further appropriate action.

Subsequent Events

- 31. The service auditor shall inquire whether management is aware of any events subsequent to the period covered by the description of the system, control objectives and related controls up to the date of the service auditor's report that could have a significant effect on user entities.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

If the service auditor is aware of a subsequent event that could have a significant effect on user entities, and information about that event is not disclosed by the service organization, the service auditor shall disclose it in the service auditor's report.

32. The service auditor has no obligation to perform any procedures regarding the description of the system, control objectives and related controls, or the suitability of design or operating effectiveness of controls after the date of the service auditor's report.

Documentation

<i>See Issues Paper – Issue I “Link with ISAE 3000 and the ISAs - Documentation”</i>
--

33. The service auditor shall prepare documentation so as to enable an experienced service auditor, having no previous connection with the engagement, to understand:
- (a) The nature, timing, and extent of the procedures performed to comply with this ISAE and applicable legal and regulatory requirements;
 - (b) The results of the procedures and the evidence obtained; and
 - (c) Significant matters arising during the engagement, and the conclusions reached thereon and significant professional judgments made in reaching those conclusions.
34. In documenting the nature, timing and extent of procedures performed, the service auditor shall record:
- (a) The identifying characteristics of the specific items or matters being tested;
 - (b) Who performed the procedures and the date such procedures were completed; and
 - (c) Who reviewed the work performed and the date and extent of such review.
35. The service auditor shall document discussions of significant matters with the service organization and others including when and with whom the discussions took place.
36. If the service auditor has identified information that is inconsistent with the service auditor's final conclusion regarding a significant matter, the service auditor shall document how the service auditor addressed the inconsistency in forming the final conclusion.
37. The service auditor shall complete the assembly of the final engagement file on a timely basis after the date of the service auditor's assurance report.
38. After the assembly of the final engagement file has been completed, the service auditor shall not delete or discard audit documentation before the end of its retention period. (Ref: Para. A24)
39. If the service auditor finds it necessary to modify existing engagement documentation or add new documentation after the assembly of the final engagement file has been completed, the service auditor shall, regardless of the nature of the modifications or additions, document:
- (a) When and by whom they were made, and (where applicable) reviewed;
 - (b) The specific reasons for making them; and

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- (c) Their effect, if any, on the auditor's conclusions.

Preparing the Service Auditor's Assurance Report

Service Auditor's Assurance Report Content

40. The service auditor's assurance report shall include the following basic elements (Ref: Para. A25):
 - (a) A title that clearly indicates the report is an independent service auditor's assurance report.
 - (b) An addressee.
 - (c) Identification of:
 - (i) The description of the system, control objectives and related controls prepared by management of the service organization, which includes:
 - an identification of the services covered by the description and the period to which the description relates; and
 - Management's assertion, which includes the matters described in paragraph 10(h)(ii) for a Type B report, or paragraph 10(i)(ii) for a Type A report.
 - (ii) If parts of the description of the system, control objectives and related controls prepared by management of the service organization are not covered by the service auditor's opinion, an identification of those parts;
 - (iii) In the rare circumstances that the description includes complementary user entity controls, a statement that the service auditor has not evaluated the operating effectiveness of complementary user entity controls, and that if complementary user entity controls are not operating effectively, the service organization's controls cannot be expected to achieve the specified objectives; and
 - (iv) Where appropriate, a statement that the description of the system, control objectives and related controls prepared by management of the service organization excludes the control objectives and related controls of relevant subservice organizations, and that the service auditor's procedures do not extend to the subservice organization.
 - (d) Identification of the criteria, and the party specifying the control objectives.
 - (e) A statement of the limitations of controls and, in the case of a Type B report, of the risk of projecting to future periods any evaluation of effectiveness.
 - (f) Identification of the purpose and intended users of the service auditor's assurance report, and, if applicable, a statement that it is restricted to specific users or for specific purposes.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- (g) A description of the service organization's and the service auditor's responsibilities, including a statement that the service organization is responsible for:
 - (i) Preparing and presenting the description of the system, control objectives and related controls, and accompanying assertions, including the completeness, accuracy and method of presentation of the description and assertions;
 - (ii) Providing the services covered by the description of the system, control objectives and related controls;
 - (iii) Identifying the control objectives (where not identified by law or regulation, or another party, e.g., a user group), and the risks that threaten their achievement; and
 - (iv) Designing, implementing and maintaining controls to achieve the identified control objectives.
- (h) A statement that the engagement was performed in accordance with ISAE 3402, "Assurance Reports on a Service Organization's Controls."
- (i) A summary of the service auditor's procedures to obtain reasonable assurance and, in the case of a Type A report, a statement that the service auditor has not performed any procedures regarding the operating effectiveness of controls and therefore no opinion is expressed thereon.
- (k) The service auditor's opinion, expressed in the positive form, on whether, in all material respects, based on suitable criteria:
 - (i) In the case of a Type B report:
 - The description presents fairly relevant aspects of the system, control objectives and related controls that had been designed and implemented throughout a specified period;
 - The controls related to the control objectives included in the description were suitably designed throughout a specified period; and
 - The controls related to the control objectives included in the description operated effectively throughout a specified period.
 - (ii) In the case of a Type A report:
 - The description presents fairly relevant aspects of the system, control objectives and related controls that had been designed and implemented as at a specified date; and
 - The controls related to the control objectives included in the description were suitably designed as at a specified date.
- (l) The date of the service auditor's assurance report.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- (m) The name of the service auditor, and the city where the service auditor maintains the office that has responsibility for the engagement.
41. In the case of a Type B report, the service auditor's assurance report shall include a separate section or attachment that describes the service auditor's tests of controls and the results thereof. In describing the tests of controls, the auditor shall indicate the nature and timing of the tests in sufficient detail to enable user auditors to determine the effect of such tests on their risk assessments. If the work of the internal audit function or an external expert is used in performing tests of controls, a description of that work and of the auditor's procedures with respect to it shall be described. If deviations have been identified, the auditor shall include:
- (a) Information about causative factors, to the extent the service auditor has identified such factors; and
 - (b) The extent of testing performed by the service auditor that led to identification of the deviations, and the number of exceptions noted.

The service auditor shall report deviations even if, on the basis of tests performed, the service auditor has concluded that the related control objective has been achieved. (Ref: Para. A26)

See Issues Paper – Issue G “Disclosure of sample sizes”

Modified Opinions

42. If the service auditor concludes that:
- (a) Management's description of the system, control objectives and related controls is not presented fairly in all material respects;
 - (b) The controls are not suitably designed to provide reasonable assurance that the specified control objectives will be achieved if the controls operate effectively;
 - (c) In the case of a Type B report, the controls did not operate effectively throughout the specified period; or
 - (d) The service auditor is unable to obtain sufficient appropriate evidence,
- the service auditor's opinion shall be modified, and the service auditor's assurance report shall contain a clear description of all the reasons for the modification. (Ref: Para. A27)

See Issues Paper – Issue E “Modified opinions”

Other Reporting Responsibilities

43. If the service auditor becomes aware of illegal acts, fraud or uncorrected errors attributable to the service organization that are not clearly trivial and may affect one or more user entities, the service auditor shall determine whether this information has been communicated appropriately to affected user entities. If the information has not been so communicated and

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

management of the service organization is unwilling to do so, the service auditor shall take appropriate action.

Application and Other Explanatory Material

Definitions (Ref: Para. 10(e))

- A1. The process referred to in the definition of “service organization’s controls” at paragraph 10 (e) invariably includes aspects of user entities’ information systems maintained by the service organization, and may also include aspects of one or more of the other components of internal control. For example, it may include aspects of the service organization’s control environment, monitoring, and control activities where they relate to the services provided. It does not, however, include controls at a service organization that are not related to the achievement of the control objectives specified in the description of the system, control objectives and related controls, e.g. controls related to the preparation of the service organization’s own financial statements. See ISA 315 (Redrafted), “Identifying and Assessing Risks of Material Misstatement Through Understanding the Entity and Its Environment” for a definition and discussion of internal control, and “controls” as they relate to a financial statement audit, including a discussion of the information system relevant to financial reporting.

Acceptance and Continuance (Ref: Para. 13(a)(iii))

- A2. A request not to include certain aspects of the service organization’s controls from the scope of the engagement may not have a reasonable justification when, e.g., the request is made because of the likelihood that the auditor’s opinion would be modified with respect to those aspects.

<i>See Issues Paper – Issue J “Scope of the engagement”</i>

Assessing the Suitability of the Criteria (Ref: Para. 17)

- A3. ISAE 3000 requires the service auditor, amongst other things, to assess the suitability of criteria, and the appropriateness of the subject matter. The subject matter is the underlying condition of interest to intended users of an assurance report. The following table identifies the subject matter and criteria for each of the opinions in Type B and Type A reports.

<i>See Issues Paper – Issue A “The Framework and ISAE 3000”</i>

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

	<i>Subject matter</i>	<i>Criteria</i>	<i>Comment</i>	
<i>Opinion about the fair presentation of the description of the system, control objectives and related controls (Type A and Type B reports)</i>	The system, controls and control objectives that are relevant to services covered by the service auditor's report.	The description is fairly presented if it: (a) Presents how the system made available to user entities has been designed and implemented to process relevant transactions including the matters identified in para 15(a); and (b) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is presented to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.	The specific wording of the criteria for this opinion may need to be tailored to be consistent with criteria established by, e.g., law or regulation, a framework such as COBIT, or user groups. There may be situations in which not all of the sub-points noted in paragraph 17(a) are required to be met by the system, e.g., when the service provided is the preparation of financial statements, or IT infrastructure. Examples of criteria for this opinion are provided in the illustrative management assertions in Appendix 3. Paragraphs A8-A11 offer further guidance on determining whether these criteria are met. (In terms of ISAE 3000, the subject matter information ² for this opinion is the description of the system, control objectives and related controls).	
<i>Opinion about suitability of design, and operating effectiveness (Type B reports)</i>	The design and operating effectiveness of those controls that are necessary to achieve control objectives relevant to services covered by the service auditor's report.	The controls are suitably designed and operating effectively if those controls necessary for achievement of relevant control objectives: (a) would, if they are operated as described throughout the specified period, provide reasonable assurance about achievement of those objectives throughout that period; and (b) operated as described during that period.	When both of the criteria for this opinion are met, controls will have provided reasonable assurance that the related control objectives were achieved throughout the specified period. (In terms of the requirements of ISAE 3000, the subject matter information ² for this opinion is the service organization's assertion that controls are suitably designed and are operating effectively).	The control objectives, which are included in the description, are part of the criteria for these opinions. The control objectives will differ from engagement to engagement. If, as part of forming the opinion on the description, the auditor concludes the stated control objectives are not fairly presented (e.g., are not complete or are not appropriate based on the services being described), then those control

² The "subject matter information" is the outcome of the evaluation or measurement of the subject matter that results from applying the criteria to the subject matter.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

<i>Opinion about suitability of design (Type A reports)</i>	The design effectiveness of controls that are necessary to achieve control objectives relevant to services covered by the service auditor's report.	The controls are suitably designed if those controls that are necessary for achievement of relevant control objectives would, if they are operated as described throughout the specified period, provide reasonable assurance about achievement of those objectives at that date.	Meeting this criterion does not, of itself, provide any assurance that the related control objectives were achieved because no assurance has been obtained about the operation of controls. (In terms of the requirements of ISAE 3000, the subject matter information for this opinion is the service organization's assertion that controls are suitably designed).	objectives would not be suitable as part of the criteria for forming an opinion on either the design or operating effectiveness of controls.
--	---	---	---	--

Using the Work of Others (Ref: Para. 18)

- A4. As used in this ISAE, "internal audit function" also includes others (by whatever name, e.g., a compliance or risk department) who work under the direction of management and perform similar activities to the internal audit function. An internal audit function may be responsible for providing analyses, evaluations, assurances, recommendations, and other information to the entity's management and those charged with governance. An internal audit function at a service organization may perform activities related to the service organization's internal control, or activities related to the services and systems, including controls, that the service organization is providing to users.
- A5. The scope and objectives of an internal audit function vary widely and depend on the size and structure of the entity and the requirements of management and those charged with governance. Internal audit function activities may include one or more of the following:
- Monitoring of the service organization's internal control or the application processing systems, including controls, provided to users. The internal audit function may be assigned specific responsibility for reviewing controls, monitoring their operation and recommending improvements thereto.
 - Examination of financial and operating information. The internal audit function may be assigned to review the means used to identify, measure, classify and report financial and operating information, and specific inquiry and other procedures into individual items including detailed testing of transactions, balances and procedures.
 - Evaluation of the economy, efficiency and effectiveness of operating activities including non-financial activities of an entity.
 - Evaluation of compliance with laws, regulations and other external requirements, and with management policies and directives and other internal requirements.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Obtaining an Understanding of the System (Ref: Para. 19)

- A6. Obtaining an understanding of relevant aspects of the system, including controls, provided by the service organization and included in the scope of the engagement, assists the service auditor in:
- Assessing whether the service organization's description of the system and controls fairly presents the system that has been designed and implemented using suitable criteria.
 - Identifying and assessing the risks of material misstatement in the description of the system, control objectives and related controls, including whether the specified control objectives are reasonable in the circumstances.
 - Determining which controls are relevant controls, and identifying and assessing the risks that relevant controls were not suitably designed, and, in the case of a Type B report, operating effectively.
- A7. Procedures to obtain this understanding may include:
- Inquiring of management, and of others within the entity who in the service auditor's judgment may have information that is likely to assist in identifying risks.
 - Observation of operations and inspection of documents, reports, printed and electronic records of transaction processing, and documentation to understand relevant aspects of the system, including controls, that is being used to provide the services described.
 - Inspecting a selection of agreements between the service organization and user entities to identify their common terms.

Obtaining Evidence Regarding the Description (Ref: Para. 20-21)

- A8. Considering the following factors may assist the service auditor in determining whether the criteria in relation to the fair presentation of the description of controls have been met:
- Does the description address all of the major aspects of the service provided (within the scope of the engagement) that could reasonably be expected to be relevant to user auditors in planning their audits of user entities' financial statements?
 - Does the description address relevant aspects of the service organization's controls?
 - Are the specified control objectives reasonable in the circumstances (see paragraph A9)?
 - Is the description presented at a level of detail that provides user auditors with sufficient information to plan the audit of the user entities' financial statements and assess the risks of material misstatement? The appropriate degree of detail of the description is equivalent to the degree of detail a user auditor would require if a service organization were not used. The description need not address every aspect of the service organization's processing or the services provided to user entities, and need not be so detailed as to potentially allow a reader to compromise security or other controls.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- Is the description prepared and presented in a manner that does not omit or distort information that may affect user auditors' decisions, e.g. does the description objectively describe any significant omissions or inaccuracies in processing of which the service auditor is aware?
- Have the controls identified in the description actually been implemented?
- Are complementary user entity controls, if any, adequately described? In most cases, the description of control objectives is worded such that the control objectives are capable of being achieved through effective operation of controls implemented by the service organization alone. In rare cases, however, the control objectives specified in the description cannot be achieved by the service organization alone because their achievement requires particular controls to be implemented by user entities. This may be the case where, e.g., the control objectives are specified by a regulatory authority. Where the description does include complementary user entity controls, the description separately identifies those controls.

See Issues Paper – Issue H “Complementary controls”

A9. Paragraph 20(a) requires the service auditor to evaluate whether the specified control objectives are reasonable in the circumstances. Considering the following factors may assist the auditor in doing this:

- Have the specified control objectives been designated by the service organization or by outside parties such as regulatory authorities, a user group or others?
- Do the specified control objectives relate to the types of assertions embodied in user entities' financial statements to which the service organization's controls could reasonably be expected to relate? Although the service auditor ordinarily will not be able to determine how a service organization's controls specifically relate to the assertions embodied in all user entities' financial statements, the service auditor's understanding of the nature of the system, including controls, and services being provided is used to identify the types of assertions to which those controls are likely to relate.
- Are the specified control objectives complete? A complete set of control objectives provides user auditors with a framework to assess the effect of the service organization's controls on the assertions in the user organizations' financial statements.

A10. The service auditor's procedures to evaluate the fair presentation of the description may include:

- Considering who the user entities are and how the services provided by the service organization are likely to affect them, e.g., the predominant type(s) of user entities, and whether user entities are regulated by government agencies.
- Review of standard contracts (if applicable) with user entities to gain an understanding of the service organization's contractual obligations.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- Observation of the procedures performed by service organization personnel.
- Review of service organization policy and procedure manuals and other systems documentation, for example, flowcharts and narratives.

A11. If services are performed by a subservice organization, the description identifies (a) those services, and (b) whether the inclusive method or the carve-out method has been used in relation to those services. If the inclusive method has been used, it is important that the description adequately differentiates between the service organization's controls and the subservice organization's controls. If the carve-out method is used, it is important that the description identify the functions that are performed by the sub-service organization, but it need not describe the detailed processing or controls at the sub-service organization.

Obtaining Evidence Regarding the Design of Controls (Ref: Para. 22)

- A12. From the viewpoint of a *user auditor*, a control is suitably designed if individually or in combination with other controls, it would, when complied with satisfactorily, provide reasonable assurance that material misstatements are prevented, or detected and corrected. A *service auditor*, however, is not aware of the circumstances at individual user entities that would determine whether or not a misstatement is material. Therefore, from the viewpoint of a service auditor, a control is suitably designed if individually or in combination with other controls, it would, when complied with satisfactorily, provide reasonable assurance that errors related to specified control objective are prevented, or detected and corrected.
- A13. A service auditor may consider using flowcharts, questionnaires, or decision tables to facilitate understanding the design of the controls.
- A14. Controls may consist of a number of integrated activities directed at the achievement of various control objectives. Consequently, where the service auditor evaluates certain activities as being ineffective in achieving a particular control objective, the existence of other activities, sometimes known as compensating controls, may nonetheless allow the service auditor to conclude that controls related to the control objective are suitably designed.

Obtaining Evidence Regarding the Effectiveness of Controls (Ref: Para. 23-24)

- A15. From the viewpoint of a *user auditor*, a control is operating effectively if individually or in combination with other controls, it provides reasonable assurance that material misstatements are prevented, or detected and corrected. A *service auditor*, however, is not aware of the circumstances at individual user entities that would determine whether or not a misstatement is material. Therefore, from the viewpoint of a service auditor, a control is operating effectively if individually or in combination with other controls, it provides reasonable assurance that errors related to specified control objective are prevented, or detected and corrected.
- A16. Obtaining an understanding of controls sufficient to opine on their design effectiveness is not sufficient evidence regarding their operating effectiveness, unless there is some automation that provides for the consistent operation of the controls as they were designed and

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

implemented. For example, obtaining information about the implementation of a manual control at a point in time does not provide evidence about operation of the control at other times. However, because of the inherent consistency of IT processing, performing procedures to determine the design of an automated control and whether it has been implemented may serve as evidence of that control's operating effectiveness, depending on the auditor's assessment and testing of controls such as those over program changes.

- A17. To be useful to user auditors, a Type B report ordinarily covers a minimum period of six months. If the period is less than six months, the service auditor may consider it appropriate to describe the reasons for the shorter period in the service auditor's assurance report. Circumstances that may necessitate a report covering a period of less than six months include when (a) the service auditor is engaged close to the date by which the report on controls is to be issued; (b) the service organization (or a particular system or application) has been in operation for less than six months; or (c) significant changes have been made to the controls and it is not practicable either to wait six months before issuing a report or to issue a report covering the system both before and after the changes.
- A18. Certain control procedures may not leave evidence of their operation that can be tested at a later date and accordingly, the service auditor may find it appropriate to test the operating effectiveness of such control procedures at various times throughout the reporting period.
- A19. The number of control operations selected as a sample for testing depends on such matters as: the frequency of the control's performance (e.g., quarterly, monthly, daily or multiple times a day), its nature (e.g., manual or automated), and its risk of failure.
- A20. Unlike in a financial statement audit, evidence from prior engagements about the satisfactory operation of controls in prior periods cannot provide a basis for a reduction in testing, even if it is supplemented with evidence obtained during the current period. This is because in a service organization engagement, the service auditor is required to provide an opinion on the effectiveness of controls throughout each period, and sufficient evidence about the operation of controls during the current period is required for the service auditor to express that opinion.
- A21. Where the service organization implemented changes to its control procedures during the period covered by the service auditor's engagement, e.g., to improve the efficiency of controls or to address identified deficiencies, the impact the superseded control procedures had on achievement of control objectives during the period may still be relevant. Where a change of controls occurs during the period, the service auditor may seek to agree with management whether it is possible for the controls to be tested before and after the change. The description of the service auditor's tests clearly states which control procedures have been tested and the period during which they were tested.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Written Representations (Ref: Para. 25-27)

A22. The written representations required by paragraph 25 are separate from, and in addition to the assertion contained in the report on controls, as described in paragraph 10 (h)(ii) for a Type B report, and paragraph 10 (i)(ii) for a Type A report.

Illegal Acts, Fraud or Uncorrected Errors (Ref: Para. 28)

A23. Appropriate action when the service auditor becomes aware of an illegal act, fraud or uncorrected error that has not been communicated appropriately to affected user entities, and management of the service organization is unwilling to do so, may include:

- Obtaining legal advice about the consequences of different courses of action.
- Communicating with those charged with governance of the service organization.
- Communicating with third parties (e.g., a regulator).
- Modifying the auditor's opinion, or adding an other matters paragraph.
- Withdrawing from the engagement where permitted in the relevant jurisdiction.

Documentation (Ref: Para. 33-39)

A24. [Proposed] ISQC 1 (Redrafted), "Quality Control for firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements" requires firms to establish policies and procedures for the retention of engagement documentation. The retention period for service audit engagements ordinarily is no shorter than five years from the date of the service auditor's report.

Preparing the Service Auditor's Assurance Report (Ref: Para. 40-42)

Service Auditor's Assurance Report Content

A25. Illustrative examples of service auditors' assurance reports and related service management assertions are contained in Appendices 2 and 3.

<i>See Issues Paper – Issue C "The service auditor's report"</i>
--

A26. In describing the nature of the service auditor's tests of controls for a Type B report, it assists readers if the service auditor's assurance report defines the types of tests performed. Illustrative definitions of common tests (inquiry, inspection, observation and re-performance) are provided in Appendix 4. It also assists readers of the service auditor's report if, in describing the extent of tests, the service auditor indicates whether the items tested represent a sample or all the items in the population.

Modified Opinions

A27. Illustrative examples of elements of modified service auditor's assurance reports are contained in Appendix 5.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Appendix 1

(Ref. Para. 10(f))

Example IT Control Objectives

The following example control objectives for IT illustrate the manner in which control objectives are ordinarily written. These example control objectives are not intended to be exhaustive or applicable to all situations. It remains the responsibility of the service organization to determine the control objectives specified in its description.

Restricting access to systems and data

- Physical access to computer networks, equipment, storage media and program documentation is restricted to authorized individuals.
- Logical access to computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorized individuals via information security tools and techniques.
- Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.

Providing integrity and resilience to the information processing environment, commensurate with the value of the information held, information processing performed and external threats

- IT processing is authorized and scheduled appropriately and deviations are identified and resolved in a timely manner.
- Data transmissions between the service organization and its counterparties are complete, accurate, timely and secure.
- Appropriate measures are implemented to counter the threat from malicious electronic attack (e.g. firewalls, anti-virus etc.).
- The physical IT equipment is maintained in a controlled environment.

Maintaining and developing systems hardware and software

- Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorized, tested, approved prior to implementation.
- Data migration or modification is authorized, tested and, once performed, reconciled back to the source data.

Monitoring compliance

- Servicing activities and controls are monitored.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Appendix 2

(Ref. Para. A25)

Example Management Assertions

The following example management assertions are for guidance only and are not intended to be exhaustive or applicable to all situations.

EXAMPLE 1: Type B Assertion for Service Organization that provides Transaction Processing Services

Management of XYZ service organization asserts that:

- (a) The accompanying description at pages *[bb-cc]* of the system, control objectives and related controls fairly presents *[the type or name of]* system made available to customers for processing their transactions throughout the *[period]* to *[date]*. The criteria we used in making this assertion were that the accompanying description:
 - (i) Presents how the system made available to user entities has been designed and implemented to process relevant transactions, including:
 - The classes of transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities.
 - The related accounting records, supporting information and specific accounts that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities.
 - How the system captures significant events and conditions, other than transactions.
 - The process used to prepare reports presented to user entities.
 - Other aspects of XYZ service organization's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to processing and reporting user entities' transactions.
 - (ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is presented to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- (b) The controls related to the control objectives included in the accompanying description were suitably designed and operated effectively throughout the *[year or other period]* to *[date]*. The criteria we used in making this assertion were that:
- (i) The controls were designed to provide reasonable assurance that the related control objectives would be achieved if the controls are operated as described; and
 - (ii) The controls were operated as described so as to provide reasonable assurance that the related control objectives were achieved throughout the specified period, based on the results of the system's operation, including monitoring procedures implemented to identify and assess the impact of any deficiencies or exceptions.

[Signature]

[Date]

[Address]

EXAMPLE 2: Type B Assertion for Service Organization that provides IT Infrastructure

Management of XYZ service organization asserts that:

- (a) The accompanying description at pages *[bb-cc]* of the system, control objectives and related controls fairly presents *IT infrastructure* system made available to customers throughout the *[year or other period]* to *[date]*. The criteria we used in making this assertion were that the accompanying description:
- (i) Presents how the *IT infrastructure* system made available to user entities has been designed and implemented, including:
 - The classes of transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities.
 - The related accounting records, supporting information and specific accounts that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities.
 - How the system captures significant events and conditions, other than transactions.
 - The process used to prepare reports presented to user entities.
 - Other aspects of XYZ service organization's control environment, risk assessment process, information system (including the related business

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

processes) and communication, control activities and monitoring controls that are relevant to processing and reporting user entities' transactions.

- (ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is presented to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.
- (b) The controls related to the control objectives included in the accompanying description were suitably designed and operated effectively throughout the *[year or other period]* to *[date]*. The criteria we used in making this assertion were that:
 - (i) The controls were designed to provide reasonable assurance that the related control objectives would be achieved if the controls are operated as described; and
 - (ii) The controls were operated as described so as to provide reasonable assurance that the related control objectives were achieved throughout the specified period, based on the results of the system's operation, including monitoring procedures implemented to identify and assess the impact of any deficiencies or exceptions.

[Signature]

[Date]

[Address]

EXAMPLE 3: Type B Assertion for Service Organization that Prepares Financial Statements

Management of XYZ service organization asserts that:

- (a) The accompanying description at pages *[bb-cc]* of the system, control objectives and related controls fairly presents the system made available to customers for preparing their financial statements throughout the *[year or other period]* to *[date]*. The criteria we used in making this assertion were that the accompanying description:
 - (i) Presents how the system made available to user entities has been designed and implemented to prepare their financial statements, including:
 - The classes of transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities.
 - The related accounting records, supporting information and specific accounts that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- How the system captures significant events and conditions, other than transactions.
 - The process used to prepare reports presented to user entities.
 - Other aspects of XYZ service organization's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to processing and reporting user entities' transactions.
- (ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is presented to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.
- (b) The controls related to the control objectives included in the accompanying description were suitably designed and operated effectively throughout the *[year or other period]* to *[date]*. The criteria we used in making this assertion were that:
- (i) The controls were designed to provide reasonable assurance that the related control objectives would be achieved if the controls are operated as described; and
 - (ii) The controls were operated as described so as to provide reasonable assurance that the related control objectives were achieved throughout the specified period, based on the results of the system's operation, including monitoring procedures implemented to identify and assess the impact of any deficiencies or exceptions.

[Signature]

[Date]

[Address]

EXAMPLE 4: Type A Assertion for Service Organization that provides Transaction Processing Services

Management of XYZ service organization asserts that:

- (a) The accompanying description at pages *[bb-cc]* of the system, control objectives and related controls fairly presents *[the type or name of]* system made available to customers for processing their transactions as at *[date]*. The criteria we used in making this assertion were that the accompanying description:
- (i) Presents how the system made available to user entities has been designed and implemented to process relevant transactions, including:
 - The classes of transactions processed.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

- The procedures, within both information technology and manual systems, by which those transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities.
 - The related accounting records, supporting information and specific accounts that are used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities.
 - How the system captures significant events and conditions, other than transactions.
 - The process used to prepare reports presented to user entities.
 - Other aspects of XYZ service organization's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to processing and reporting user entities' transactions.
- (ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is presented to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.
- (b) The controls related to the control objectives included in the accompanying description were suitably designed as at *[date]*. The criterion we used in making this assertion was that the controls were designed to provide reasonable assurance that the related control objectives would be achieved if the controls are operated as described.

[Signature]

[Date]

[Address]

IAASB CAG REFERENCE PAPER
IAASB CAG Agenda (September 2007)
Agenda Item M.2
Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Appendix 3
(Ref. Para. A25)

Example Service Auditor's Assurance Reports

The following example reports are for guidance only and are not intended to be exhaustive or applicable to all situations.

EXAMPLE 1: Type B Service Auditor's Assurance Report

**Independent Service Auditor's Assurance Report on
the Description of Controls and their Design and Operation**

To: XYZ Service Organization

Scope

We have conducted an assurance engagement to report on XYZ Service Organization's description at pages [bb-cc] of [the type or name of] system made available to customers for processing their transactions throughout the [year or other period] to [date] (the description), and on the design and operation of controls related to the control objectives included in the description.

Management's Responsibilities

Management of XYZ Service Organization is responsible for preparing and presenting the description and accompanying assertions at page [aa], including the completeness, accuracy and method of presentation of the description and assertions, providing the services covered by the description, identifying the control objectives and the risks that threaten their achievement, and designing, implementing and maintaining controls to achieve the identified control objectives.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description, and on the design and operation of controls related to the control objectives included in that description, based on our engagement. We conducted our engagement in accordance with International Standard on Assurance Engagements ISAE 3402, "Assurance Reports on a Service Organization's Controls" issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements, and plan and perform our engagement to obtain reasonable assurance whether the description is free from material misstatement and the controls are suitably designed and operating effectively in all material respects.

An assurance engagement on the description, design and operation of a service organization's controls involves performing procedures to obtain evidence about the disclosures in the description

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

of the system, control objectives and related controls, and the design and operation of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the description, and the risks of material deficiencies in design or operation of the controls, whether due to fraud or error. An assurance engagement of this type also includes evaluating the overall presentation of the description, and the suitability of the objectives included in therein.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Internal Controls at a Service Organization

Because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters, and is subject to the inherent limitations, outlined above. The criteria we used in forming our opinion were those described in management's assertion at page [aa]. In our opinion in all material respects:

- (a) The description presents fairly relevant aspects of the system, control objectives and related controls that had been designed and implemented throughout the [year or other period] to [date], and
- (b) The controls related to the control objectives included in the description were suitably designed throughout the [year or other period] to [date];
- (c) The controls related to the control objectives included in the description operated effectively throughout the [year or other period] to [date].

Description of Tests of Controls

The specific controls that were tested and the nature, timing and results of those tests are listed on pages [yy-zz].

Intended Users and Purpose

This report and the description of tests of controls on pages [yy-zz] are intended only for user entities and their auditors to be taken into consideration along with other information about controls at user entities, when assessing the risks of material misstatements of user entities' financial statements.

[Service auditor's signature]

[Date of the service auditor's assurance report]

[Service auditor's address]

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

EXAMPLE 2: Type A Service Auditor's Assurance Report

Independent Service Auditor's Assurance Report on the Description of Controls and their Design

To: XYZ Service Organization

Scope

We have conducted an assurance engagement to report on XYZ Service Organization's description at pages [bb-cc] of [the type or name of] system made available to customers for processing their transactions as at [date] (the description), and on the design of controls related to the control objectives included in the description.

Management's Responsibilities

Management of XYZ Service Organization is responsible for preparing and presenting the description and accompanying assertions at page [aa], including the completeness, accuracy and method of presentation of the description and the assertions, providing the services covered by the description, identifying the control objectives and the risks that threaten their achievement, and designing, implementing and maintaining controls to achieve the identified control objectives.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description, and on the design of controls related to the control objectives included in that description, based on our engagement. We conducted our engagement in accordance with International Standard on Assurance Engagements ISAE 3402, "Assurance Reports on a Service Organization's Controls" issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements, and plan and perform our engagement to obtain reasonable assurance whether the description is free from material misstatement and the controls are suitably designed in all material respects.

An assurance engagement on the description and design of a service organization's controls involves performing procedures to obtain evidence about the disclosures in the description of the system, control objectives and related controls, and the design of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the description, and the risks of material deficiencies in design of the controls, whether due to fraud or error. An assurance engagement of this type also includes evaluating the overall presentation of the description, and the suitability of the objectives included therein.

We did not perform any procedures regarding the operating effectiveness of controls included in the description, and accordingly do not express an opinion thereon.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Internal Controls at a Service Organization

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions.

Opinion

Our opinion has been formed on the basis of the matters, and is subject to the inherent limitations, outlined above. The criteria we used in forming our opinion were those described in management's assertion at page [aa]. In our opinion, in all material respects:

- (a) The description presents fairly relevant aspects of the system, control objectives and related controls that had been designed and implemented as at [date], and
- (b) The controls related to the control objectives included in the description were suitably designed as at [date].

Intended Users and Purpose

This report is intended only for user entities and their auditors to be taken into consideration, along with other information including information about controls at user entities themselves, when assessing the risks of material misstatements of user entities' financial statements.

[Service auditor's signature]

[Date of the service auditor's assurance report]

[Service auditor's address]

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Appendix 4

(Ref. Para. A26)

Illustrative descriptions of enquiry, inspection, observation and reperformance

The following illustrative descriptions are for guidance only and are not intended to be exhaustive or applicable to all situations.

Enquiry

Inquiry of appropriate [*entity*] personnel. Inquiries seeking relevant information or representation from personnel were performed to obtain, among other things:

- Knowledge, additional information and affirmation regarding controls; and
- Corroborating evidence of the operation of controls.

Inspection

Inspection of documents and records indicating performance of controls, including:

- Inspection of reconciliations and management reports that age and/or quantify reconciling items to assess whether balances and reconciling items appear to be properly monitored, controlled and resolved on a timely basis, as required by the related control;
- Examination of source documentation and authorizations related to selected transactions processed;
- Examination of documents or records for evidence of performance such as the existence of initials or signatures; and
- Inspection of [*entity's*] systems documentation, such as operations, manuals, flow charts and job descriptions.

Observation

Observation of the application or existence of specific controls as described.

Reperformance

Reperformance of the controls to check the accuracy of their operation, including:

- Obtaining evidence of the arithmetical accuracy and correct processing of transactions by performing independent calculations; and
- Reproducing the matching of various system records by independently matching the same records and comparing reconciling items to reconciliations prepared by the service organization.

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Appendix 5

(Ref. Para. A27)

Example Modified Service Auditor's Assurance Report

The following examples of modified service auditor's assurance reports are for guidance only and are not intended to be exhaustive or applicable to all situations.

EXAMPLE 1: Qualified opinion – management's description of the system, control objectives and related controls is not presented fairly in all material respects

“...

Service Auditor's Responsibilities

...

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Basis for Qualified Opinion

The accompanying system description states at page [mn] that XYZ Service Organization uses operator identification numbers and passwords to prevent unauthorized access to the system. Based on inquiries of staff personnel and observation of activities, we have determined that such procedures are employed in Applications A and B but are not required to access the system in Applications C and D.

Qualified Opinion

Our opinion has been formed on the basis of the matters, and is subject to the inherent limitations, outlined above. The criteria we used in forming our opinion were those described in management's assertion at page [aa]. In our opinion, except for the matter described in the Basis for Qualified Opinion paragraph:

(a) ...”

EXAMPLE 2 Qualified opinion – the controls are not suitably designed to provide reasonable assurance that the specified control objectives will be achieved if the controls operate effectively

“...

Service Auditor's Responsibilities

...

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Basis for Qualified Opinion

As discussed at page [mn] of the accompanying description, from time to time XYZ Service Organization makes changes in application programs to correct deficiencies or to enhance capabilities. The procedures followed in determining whether to make changes, in designing the changes and in implementing them do not include review and approval by authorized individuals who are independent from those involved in making the changes. There are also no specified requirements to test such changes or provide test results to an authorized reviewer prior to implementing the changes.

Qualified Opinion

Our opinion has been formed on the basis of the matters, and is subject to the inherent limitations, outlined above. The criteria we used in forming our opinion were those described in management's assertion at page [aa]. In our opinion, except for the matter described in the Basis for Qualified Opinion paragraph:

(a) ...”

EXAMPLE 3 Qualified opinion – the controls did not operate effectively throughout the specified period (Type B report only)

“...

Service Auditor's Responsibilities

...

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Basis for Qualified Opinion

XYZ Service Organization states in its description that it has automated controls in place to reconcile loan payments received with the output generated. However, as noted at page [mn] of the description, this control was not operating effectively during the period from dd/mm/yyyy to dd/mm/yyyy due to a programming error. This resulted in the non-achievement of the control objective "Controls provide reasonable assurance that loan payments received are properly recorded" during the period from dd/mm/yyyy to dd/mm/yyyy. Management implemented a change to the program performing the calculation as of [date], and our tests indicate that it was operating effectively during the period from dd/mm/yyyy to dd/mm/yyyy.

Qualified Opinion

IAASB CAG REFERENCE PAPER

IAASB CAG Agenda (September 2007)

Agenda Item M.2

Service Organizations – ISAE 3402 DRAFT – September 2007 IAASB Agenda Item 10-A

Our opinion has been formed on the basis of the matters, and is subject to the inherent limitations, outlined above. The criteria we used in forming our opinion were those described in management's assertion at page [aa]. In our opinion, except for the matter described in the Basis for Qualified Opinion paragraph:

(a) ...”

EXAMPLE 4 Qualified opinion – the service auditor is unable to obtain sufficient appropriate evidence

“...

Service Auditor's Responsibilities

...

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

Basis for Qualified Opinion

XYZ Service Organization states in its description that it has automated controls in place to reconcile loan payments received with the output generated. However, management informed us that electronic records of the performance of this reconciliation for the period dd/mm/yyyy till dd/mm/yyyy were deleted as a result of a computer processing error, and we were therefore unable to test the operation of this control for that period. Consequently, we were unable to determine whether the control objective "Controls provide reasonable assurance that loan payments received are properly recorded" operated effectively during the period from dd/mm/yyyy to dd/mm/yyyy.

Qualified Opinion

Our opinion has been formed on the basis of the matters, and is subject to the inherent limitations, outlined above. The criteria we used in forming our opinion were those described in management's assertion at page [aa]. In our opinion, except for the matter described in the Basis for Qualified Opinion paragraph:

(a) ...”