

Agenda Item 6.2
AUASB Meeting 8 June 2010
Clean Version

ASAE 3402
(June 2010)

**Standard on Assurance
Engagements ASAE 3402**
*Assurance Reports on
Controls at a Service
Organisation*

Issued by the **Auditing and Assurance Standards Board**



Australian Government

Auditing and Assurance Standards Board

Obtaining a Copy of this Standard on Assurance Engagements

This Standard on Assurance Engagements is available on the AUASB website: www.auasb.gov.au

Contact Details

Auditing and Assurance Standards Board
Level 7
600 Bourke Street
Melbourne Victoria 3000
AUSTRALIA

Phone: (03) 8080 7400
Fax: (03) 8080 7450
E-mail: enquiries@auasb.gov.au

Postal Address:
PO Box 204
Collins Street West
Melbourne Victoria 8007
AUSTRALIA

COPYRIGHT

© 2010 Auditing and Assurance Standards Board (AUASB). The text, graphics and layout of this Standard on Assurance Engagements are protected by Australian copyright law and the comparable law of other countries. Reproduction within Australia in unaltered form (retaining this notice) is permitted for personal and non-commercial use subject to the inclusion of an acknowledgment of the source. Requests and enquiries concerning reproduction and rights for commercial purposes within Australia should be addressed to the Executive Director, Auditing and Assurance Standards Board, PO Box 204, Collins Street West, Melbourne Victoria 8007. Otherwise, no part of the Standard on Assurance Engagements may be reproduced, stored or transmitted in any form or by any means without the prior written permission of the AUASB except as permitted by law.

ISSN 1834-4860

ASAE 3402

- 2 -

CONTENTS

PREFACE

AUTHORITY STATEMENT

	<i>Paragraphs</i>
Application	Aus 0.1
Operative Date	Aus 0.2
Introduction	
Scope of this Standard on Assurance Engagements.....	1-Aus 6.1
Effective Date	7
Objectives	8
Definitions	9
Requirements	
ASAE 3000	10
Ethical Requirements	11
Management and Those Charged with Governance	12
Acceptance and Continuance	13-14
Assessing the Suitability of the Criteria	15-18
Materiality	19
Obtaining an Understanding of the Service Organisation's System	20
Obtaining Evidence Regarding the Description	21-22
Obtaining Evidence Regarding Design of Controls	23
Obtaining Evidence Regarding Operating Effectiveness of Controls	24-29
The Work of an Internal Audit Function	30-37
Written Representations	38-40
Other Information	41-42
Subsequent Events	43-44
Documentation	45-52

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Preparing the Service Auditor's Assurance Report	53-55
Other Communication Responsibilities	56
Application and Other Explanatory Material	
Scope of this Standard on Assurance Engagements	A1-A2
Definitions	A3-A4
Ethical Requirements	Aus A5.1
Management and Those Charged with Governance	A6
Acceptance and Continuance	A7-Aus A12.1
Assessing the Suitability of the Criteria	A13-A15
Materiality	A16-A18
Obtaining an Understanding of the Service Organisation's System	A19-A20
Obtaining Evidence Regarding the Description	A21-A24
Obtaining Evidence Regarding Design of Controls	A25-A27
Obtaining Evidence Regarding Operating Effectiveness of Controls	A28-A36
The Work of an Internal Audit Function	A37-A41
Written Representations	A42-A43
Other Information	A44-A45
Documentation	A46
Preparing the Service Auditor's Assurance Report	A47-A52
Other Communication Responsibilities	A53
Conformity with International Standards on Assurance Engagements	
[Aus] Appendix 0A: Example Engagement Letter	
[Aus] Appendix 0B: Example Representation Letter	
Appendix 1: Example Service Organisation's Assertions	
[Aus] Appendix 1A: Illustrative Example of a Service Organisation's Description of the System Accompanying XYZ Service Organisation Management's Assertion	

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Appendix 2: Example Service Auditor's Assurance Reports

Appendix 3: Example Modified Service Auditor's Assurance
Reports

Draft

PREFACE

Reasons for Issuing Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation*

The AUASB as an independent statutory board of the Australian Government established under section 227A of the *Australian Securities and Investments Commission Act 2001*, as amended (ASIC Act). Under section 227B of the ASIC Act the AUASB may formulate Assurance Standards for purposes other than the corporations legislation.

Under the Strategic Direction given to the AUASB by the Financial Reporting Council (FRC), the AUASB is required to have regard to any programme initiated by the International Auditing and Assurance Standards Board (IAASB) for the development, revision and enhancement of its standards and to make appropriate consequential amendments to the Australian Auditing and Assurance Standards. Accordingly, the AUASB has decided to issue ASAE 3402 using the equivalent International Standard on Assurance Engagements ISAE 3402 *Assurance Reports on Controls at a Service Organization*.

Main Features

This Standard on Assurance Engagements (ASAE) establishes requirements and provides application and other explanatory material regarding the assurance practitioner's responsibilities when providing a report for use by user entities and their auditors, on the controls at a service organisation that provides a service to user entities that is likely to be relevant to user entities' internal control as it relates to financial reporting.

Draft

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

AUTHORITY STATEMENT

The Auditing and Assurance Standards Board (AUASB) formulates this Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation* pursuant to section 227B of the *Australian Securities and Investments Commission Act 2001*.

This Standard on Assurance Engagements is to be read in conjunction with ASA 100 *Preamble to AUASB Standards*, which sets out the intentions of the AUASB on how the AUASB Standards are to be understood, interpreted and applied.

Dated: 8 June 2010

M H Kelsall
Chairman - AUASB

STANDARD ON ASSURANCE ENGAGEMENTS ASAE 3402

Assurance Reports on Controls at a Service Organisation

Application

Aus 0.1 This Standard on Assurance Engagements applies to an assurance engagement to provide an assurance report for use by user entities and their auditors on the controls at a service organisation.

Operative Date

Aus 0.2 This Standard on Assurance Engagements is operative for service auditors' assurance reports covering periods commencing on or after 1 July 2010. Early adoption is permitted.

Introduction

Scope of this Standard on Assurance Engagements

1. This Standard on Assurance Engagements deals with assurance engagements undertaken by an assurance practitioner^{1*} to provide a report for use by user entities and their auditors, on the controls at a service organisation that provides a service to user entities that is likely to be relevant to user entities' internal control as it relates to financial reporting. It complements ASA 402,² in that reports prepared in accordance with this standard are capable of providing appropriate evidence under ASA 402. (Ref: Para. A1)
2. The *Framework for Assurance Engagements* (the Assurance Framework) states that an assurance engagement may be a "reasonable assurance" engagement or a "limited assurance" engagement; that an assurance engagement may be either an

¹ [Footnote deleted by the AUASB. Refer following footnote "**"]
^{*} See ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports, Other Financial Information, and Other Assurance Engagements*, Para. Aus 12.2 and ASA 220 *Quality Control for an Audit of a Financial Report and Other Historical Financial Information*, Para. Aus 7.1.

² See ASA 402 *Audit Considerations Relating to an Entity Using a Service Organisation*.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

“assertion-based” engagement or a “direct reporting” engagement; and, that the assurance conclusion for an assertion-based engagement can be worded either in terms of the responsible party’s assertion or directly in terms of the subject matter and the criteria.³ This standard only deals with assertion-based engagements that convey reasonable assurance, with the assurance conclusion worded directly in terms of the subject matter and the criteria.⁴

3. [Deleted by the AUASB. Refer Aus 3.1].

Aus 3.1 This standard applies only when the service organisation is responsible for, or otherwise able to make an assertion about, the suitable design of controls as they relate to financial reporting. This standard does not deal with assurance engagements:

- (a) To report only on whether controls at the service organisation operated as described without reporting on the suitability of design of controls, or
- (b) Which do not report on controls which are likely to be relevant to user entities’ internal control as it relates to financial reporting (for example, reports only on controls that affect user entities’ production or quality control).

This standard, however, provides some guidance for such engagements carried out under ASAE 3000.⁵ (Ref: Para. A2)

4. In addition to issuing an assurance report on controls, a service auditor may also be engaged to provide reports such as the following, which are not dealt with in this standard:

- (a) A report on a user entity’s transactions or balances maintained by a service organisation; or
- (b) An agreed-upon procedures report on controls at a service organisation.

³ See Assurance Framework.

⁴ See paragraphs 13 and 53(k) of this standard.

⁵ See ASAE 3000 *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Relationship with Other Professional Pronouncements

5. The performance of assurance engagements other than audits or reviews of historical financial information requires the service auditor to comply with ASAE 3000. ASAE 3000 includes requirements in relation to such topics as engagement acceptance, planning, evidence, and documentation that apply to all assurance engagements, including engagements in accordance with this standard. This standard expands on how ASAE 3000 is to be applied in a reasonable assurance engagement to report on controls at a service organisation. The Assurance Framework, which defines and describes the elements and objectives of an assurance engagement, provides the context for understanding this standard and ASAE 3000.

6. [Deleted by the AUASB. Refer Aus 6.1].⁶

Aus 6.1 Compliance with ASAE 3000 requires, among other things, that the service auditor comply with the fundamental ethical principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour, and implement quality control procedures that are applicable to the individual engagement.*

Effective Date

7. [Deleted by the AUASB. Refer Aus 0.2]

Objectives

8. The objectives of the service auditor are:

- (a) To obtain reasonable assurance about whether, in all material respects, based on suitable criteria:
 - (i) The service organisation's description of its system fairly presents the system as designed and implemented throughout the specified period (or in the case of a type 1 report, as at a specified date);
 - (ii) The controls related to the control objectives stated in the service organisation's description of its system were suitably designed throughout the

⁶ [Footnote deleted by the AUASB]

* See ASAE 3000, paragraphs 9 and 12.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

specified period (or in the case of a type 1 report, as at a specified date); and

- (iii) Where included in the scope of the engagement, the controls operated effectively to provide reasonable assurance that the control objectives stated in the service organisation's description of its system were achieved throughout the specified period.
- (b) To report on the matters in (a) above in accordance with the service auditor's findings.

Definitions

9. For purposes of this Standard on Assurance Engagements, the following terms have the meanings attributed below:
- (a) Carve-out method means method of dealing with the services provided by a subservice organisation, whereby the service organisation's description of its system includes the nature of the services provided by a subservice organisation, but that subservice organisation's relevant control objectives and related controls are excluded from the service organisation's description of its system and from the scope of the service auditor's engagement. The service organisation's description of its system and the scope of the service auditor's engagement include controls at the service organisation to monitor the effectiveness of controls at the subservice organisation, which may include the service organisation's review of an assurance report on controls at the subservice organisation.
 - (b) Complementary user entity controls means controls that the service organisation assumes, in the design of its service, will be implemented by user entities, and which, if necessary to achieve control objectives stated in the service organisation's description of its system, are identified in that description.
 - (c) Control objective means the aim or purpose of a particular aspect of controls. Control objectives relate to risks that controls seek to mitigate.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (d) Controls at the service organisation means controls over the achievement of a control objective that is covered by the service auditor's assurance report. (Ref: Para. A3)
- (e) Controls at a subservice organisation means controls at a subservice organisation to provide reasonable assurance about the achievement of a control objective.
- (f) Criteria means benchmarks used to evaluate or measure a subject matter including, where relevant, benchmarks for presentation and disclosure.
- (g) Inclusive method means method of dealing with the services provided by a subservice organisation, whereby the service organisation's description of its system includes the nature of the services provided by a subservice organisation, and that subservice organisation's relevant control objectives and related controls are included in the service organisation's description of its system and in the scope of the service auditor's engagement. (Ref: Para. A4)
- (h) Internal audit function means an appraisal activity established or provided as a service to the service organisation. Its functions include, amongst other things, examining, evaluating and monitoring the adequacy and effectiveness of internal control.
- (i) Internal auditors means those individuals who perform the activities of the internal audit function. Internal auditors may belong to an internal audit department or equivalent function.
- (j) Report on the description and design of controls at a service organisation (referred to in this standard as a "type 1 report") means a report that comprises:
 - (i) The service organisation's description of its system;
 - (ii) A written assertion by the service organisation that, in all material respects, and based on suitable criteria:

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- a. The description fairly presents the service organisation's system as designed and implemented as at the specified date; and
- b. The controls related to the control objectives stated in the service organisation's description of its system were suitably designed as at the specified date; and
- (iii) A service auditor's assurance report that conveys reasonable assurance about the matters in (ii)a.-b. above.
- (k) Report on the description, design and operating effectiveness of controls at a service organisation (referred to in this standard as a "type 2 report") means a report that comprises:
 - (i) The service organisation's description of its system;
 - (ii) A written assertion by the service organisation that, in all material respects, and based on suitable criteria:
 - a. The description fairly presents the service organisation's system as designed and implemented throughout the specified period;
 - b. The controls related to the control objectives stated in the service organisation's description of its system were suitably designed throughout the specified period; and
 - c. The controls related to the control objectives stated in the service organisation's description of its system operated effectively throughout the specified period; and

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (iii) A service auditor's assurance report that:
 - a. Conveys reasonable assurance about the matters in (ii)a.-c. above; and
 - b. Includes a description of the tests of controls and the results thereof.
- (l) Service auditor means an assurance practitioner who, at the request of the service organisation, provides an assurance report on controls at a service organisation.
- (m) Service organisation means a third-party organisation (or segment of a third-party organisation) that provides services to user entities that are likely to be relevant to user entities' internal control as it relates to financial reporting.
- (n) Service organisation's system (or the system) means the policies and procedures designed and implemented by the service organisation to provide user entities with the services covered by the service auditor's assurance report. The service organisation's description of its system includes identification of: the services covered; the period, or in the case of a type 1 report, the date, to which the description relates; control objectives; and related controls.
- (o) Service organisation's assertion means the written assertion about the matters referred to in paragraph 9(k)(ii) (or paragraph 9(j)(ii) in the case of a type 1 report).
- (p) Subservice organisation means a service organisation used by another service organisation to perform some of the services provided to user entities that are likely to be relevant to user entities' internal control as it relates to financial reporting.
- (q) Test of controls means a procedure designed to evaluate the operating effectiveness of controls in achieving the control objectives stated in the service organisation's description of its system.
- (r) User auditor means an auditor who audits and reports on the financial report/statements of a user entity.⁷

⁷ [Footnote deleted by the AUASB. See Aus 9.1]

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- Aus 9.1 In the case of a subservice organisation, the service auditor of a service organisation that uses the services of the subservice organisation is also a user auditor.
- (s) User entity means an entity that uses a service organisation.

Requirements

ASAE 3000

10. The service auditor shall not represent compliance with this standard unless the service auditor has complied with the requirements of this standard and ASAE 3000.

Ethical Requirements

11. The service auditor shall comply with relevant ethical requirements, including those pertaining to independence, relating to assurance engagements.* (Ref: Para. Aus A5.1)

Management and Those Charged with Governance

12. Where this standard requires the service auditor to enquire of, request representations from, communicate with, or otherwise interact with the service organisation, the service auditor shall determine the appropriate person(s) within the service organisation's management or governance structure with whom to interact. This shall include consideration of which person(s) have the appropriate responsibilities for and knowledge of the matters concerned.
(Ref: Para. A6)

Acceptance and Continuance

13. Before agreeing to accept, or continue, an engagement, the service auditor shall:
- (a) Determine whether:
- (i) The service auditor has the capabilities and competence to perform the engagement;
(Ref: Para. A7)

* See ASA 102 *Compliance with Ethical Requirements when Performing Audits, Reviews and Other Assurance Engagements*.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (ii) The criteria to be applied by the service organisation to prepare the description of its system will be suitable and available to user entities and their auditors; and
 - (iii) The scope of the engagement and the service organisation's description of its system will not be so limited that they are unlikely to be useful to user entities and their auditors.
- (b) Obtain the agreement of the service organisation that it acknowledges and understands its responsibility:
- (i) For the preparation of the description of its system, and accompanying service organisation's assertion, including the completeness, accuracy and method of presentation of that description and assertion; (Ref: Para. A8)
 - (ii) To have a reasonable basis for the service organisation's assertion accompanying the description of its system; (Ref: Para. A9)
 - (iii) For stating in the service organisation's assertion the criteria it used to prepare the description of its system;
 - (iv) For stating in the description of its system:
 - a. The control objectives; and,
 - b. Where they are specified by law or regulation, or another party (for example, a user group or a professional body), the party who specified them;
 - (v) For identifying the risks that threaten achievement of the control objectives stated in the description of its system, and designing and implementing controls to provide reasonable assurance that those risks will not prevent achievement of the control objectives stated in the description of its system, and therefore that the stated control objectives will be achieved; and (Ref: Para. A10)

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (vi) To provide the service auditor with:
 - a. Access to all information, such as records, documentation and other matters, including service level agreements, of which the service organisation is aware that is relevant to the description of the service organisation's system and the accompanying service organisation's assertion;
 - b. Additional information that the service auditor may request from the service organisation for the purpose of the assurance engagement; and
 - c. Unrestricted access to persons within the service organisation from whom the service auditor determines it necessary to obtain evidence.

Acceptance of a Change in the Terms of the Engagement

14. If the service organisation requests a change in the scope of the engagement before the completion of the engagement, the service auditor shall be satisfied that there is a reasonable justification for the change. (Ref: Para. A11-Aus A12.1)

Assessing the Suitability of the Criteria

15. As required by ASAE 3000, the service auditor shall assess whether the service organisation has used suitable criteria in preparing the description of its system, in evaluating whether controls are suitably designed, and, in the case of a type 2 report, in evaluating whether controls are operating effectively.⁸
16. In assessing the suitability of the criteria to evaluate the service organisation's description of its system, the service auditor shall determine if the criteria encompass, at a minimum:
- (a) Whether the description presents how the service organisation's system was designed and implemented, including, as appropriate:

⁸ See ASAE 3000, paragraph 35.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (i) The types of services provided, including, as appropriate, classes of transactions processed;
 - (ii) The procedures, within both information technology and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities;
 - (iii) The related records and supporting information, including, as appropriate, 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 and other information prepared for user entities;
 - (iv) How the service organisation's system deals with significant events and conditions, other than transactions;
 - (v) The process used to prepare reports and other information for user entities;
 - (vi) The specified control objectives and controls designed to achieve those objectives;
 - (vii) Complementary user entity controls contemplated in the design of the controls; and
 - (viii) Other aspects of the service organisation's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the services provided. (Ref: Para. A15)
- (b) In the case of a type 2 report, whether the description includes relevant details of changes to the service organisation's system during the period covered by the description.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (c) Whether the description omits or distorts information relevant to the scope of the service organisation's system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the service organisation's system that each individual user entity and its auditor may consider important in its particular environment.
17. In assessing the suitability of the criteria to evaluate the design of controls, the service auditor shall determine if the criteria encompass, at a minimum, whether:
- (a) The service organisation has identified the risks that threaten achievement of the control objectives stated in the description of its system; and
 - (b) The controls identified in that description would, if operated as described, provide reasonable assurance that those risks do not prevent the stated control objectives from being achieved.
18. In assessing the suitability of the criteria to evaluate the operating effectiveness of controls in providing reasonable assurance that the stated control objectives identified in the description will be achieved, the service auditor shall determine if the criteria encompass, at a minimum, whether the controls were consistently applied as designed throughout the specified period. This includes whether manual controls were applied by individuals who have the appropriate competence and authority. (Ref: Para. A13-A14)

Materiality

19. When planning and performing the engagement, the service auditor shall consider materiality with respect to the fair presentation of the description, the suitability of the design of controls and, in the case of a type 2 report, the operating effectiveness of controls. (Ref: Para. A16-A18)

Obtaining an Understanding of the Service Organisation's System

20. The service auditor shall obtain an understanding of the service organisation's system, including controls that are included in the scope of the engagement. (Ref: Para. A19-A20)

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Obtaining Evidence Regarding the Description

21. The service auditor shall obtain and read the service organisation's description of its system, and shall evaluate whether those aspects of the description included in the scope of the engagement are fairly presented, including whether: (Ref: Para. A21-A22)
- (a) Control objectives stated in the service organisation's description of its system are reasonable in the circumstances; (Ref: Para. A23)
 - (b) Controls identified in that description were implemented;
 - (c) Complementary user entity controls, if any, are adequately described; and
 - (d) Services performed by a subservice organisation, if any, are adequately described, including whether the inclusive method or the carve-out method has been used in relation to them.
22. The service auditor shall determine, through other procedures in combination with enquiries, whether the service organisation's system has been implemented. Those other procedures shall include observation, and inspection of records and other documentation, of the manner in which the service organisation's system operates and controls are applied. (Ref: Para. A24)

Obtaining Evidence Regarding Design of Controls

23. The service auditor shall determine which of the controls at the service organisation are necessary to achieve the control objectives stated in the service organisation's description of its system, and shall assess whether those controls were suitably designed. This determination shall include: (Ref: Para. A25-A27)
- (a) Identifying the risks that threaten the achievement of the control objectives stated in the service organisation's description of its system; and
 - (b) Evaluating the linkage of controls identified in the service organisation's description of its system with those risks.

Obtaining Evidence Regarding Operating Effectiveness of Controls

24. When providing a type 2 report, the service auditor shall test those controls that the service auditor has determined are necessary to achieve the control objectives stated in the service organisation's description of its system, and assess their operating effectiveness throughout the period. Evidence obtained in prior engagements about the satisfactory operation of controls in prior periods does not provide a basis for a reduction in testing, even if it is supplemented with evidence obtained during the current period. (Ref: Para. A28-A32)
25. When designing and performing tests of controls, the service auditor shall:
- (a) Perform other procedures in combination with enquiry to obtain evidence about:
 - (i) How the control was applied;
 - (ii) The consistency with which the control was applied; and
 - (iii) By whom or by what means the control was applied;
 - (b) Determine whether 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
(Ref: Para. A33-A34)
 - (c) Determine means of selecting items for testing that are effective in meeting the objectives of the procedure.
(Ref: Para. A35-A36)
26. When determining the extent of tests of controls, the service auditor shall consider matters including the characteristics of the population to be tested, which includes the nature of controls, the frequency of their application (for example, monthly, daily, a number of times per day), and the expected rate of deviation.

Sampling

27. When the service auditor uses sampling, the service auditor shall:
(Ref: Para. A35-A36)

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (a) Consider the purpose of the procedure and the characteristics of the population from which the sample will be drawn when designing the sample;
- (b) Determine a sample size sufficient to reduce sampling risk to an appropriately low level;
- (c) Select items for the sample in such a way that each sampling unit in the population has a chance of selection;
- (d) If a designed procedure is not applicable to a selected item, perform the procedure on a replacement item; and
- (e) If unable to apply the designed procedures, or suitable alternative procedures, to a selected item, treat that item as a deviation.

Nature and Cause of Deviations

28. The service auditor shall investigate the nature and cause of any deviations identified and shall 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 or of other controls is necessary to reach a conclusion on whether the controls relative to a particular control objective are operating effectively throughout the specified period; or (Ref: Para. A25)
 - (c) The testing that has been performed provides an appropriate basis for concluding that the control did not operate effectively throughout the specified period.
29. In the extremely rare circumstances when the service auditor considers a deviation discovered in a sample to be an anomaly and no other controls have been identified that allow the service auditor to conclude that the relevant control objective is operating effectively throughout the specified period, the service auditor shall obtain a high degree of certainty that such deviation is not representative of the population. The service auditor shall obtain this degree of certainty by performing additional procedures to

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

obtain sufficient appropriate evidence that the deviation does not affect the remainder of the population.

The Work of an Internal Audit Function⁹

Obtaining an Understanding of the Internal Audit Function

30. If the service organisation has an internal audit function, the service auditor shall obtain an understanding of the nature of the responsibilities of the internal audit function and of the activities performed in order to determine whether the internal audit function is likely to be relevant to the engagement. (Ref: Para. A37)

Aus 30.1 This standard does not deal with instances when individual internal auditors provide direct assistance to the service auditor in carrying out assurance procedures.

Determining Whether and to What Extent to Use the Work of the Internal Auditors

31. The service auditor shall determine:
- (a) Whether the work of the internal auditors is likely to be adequate for purposes of the engagement; and
 - (b) If so, the planned effect of the work of the internal auditors on the nature, timing or extent of the service auditor's procedures.
32. In determining whether the work of the internal auditors is likely to be adequate for purposes of the engagement, the service auditor shall evaluate:
- (a) The objectivity of the internal audit function;
 - (b) The technical competence of the internal auditors;
 - (c) Whether the work of the internal auditors is likely to be carried out with due professional care; and
 - (d) Whether there is likely to be effective communication between the internal auditors and the service auditor.

⁹ [Footnote deleted by the AUASB. Refer Aus 30.1]

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

33. In determining the planned effect of the work of the internal auditors on the nature, timing or extent of the service auditor's procedures, the service auditor shall consider: (Ref: Para. A38)
- (a) The nature and scope of specific work performed, or to be performed, by the internal auditors;
 - (b) The significance of that work to the service auditor's conclusions; and
 - (c) The degree of subjectivity involved in the evaluation of the evidence gathered in support of those conclusions.

Using the Work of the Internal Audit Function

34. In order for the service auditor to use specific work of the internal auditors, the service auditor shall evaluate and perform procedures on that work to determine its adequacy for the service auditor's purposes. (Ref: Para. A39)
35. To determine the adequacy of specific work performed by the internal auditors for the service auditor's purposes, the service auditor shall evaluate whether:
- (a) The work was performed by internal auditors having adequate technical training and proficiency;
 - (b) The work was properly supervised, reviewed and documented;
 - (c) Adequate evidence has been obtained to enable the internal auditors to draw reasonable conclusions;
 - (d) Conclusions reached are appropriate in the circumstances and any reports prepared by the internal auditors are consistent with the results of the work performed; and
 - (e) Exceptions relevant to the engagement or unusual matters disclosed by the internal auditors are properly resolved.

Effect on the Service Auditor's Assurance Report

36. If the work of the internal audit function has been used, the service auditor shall make no reference to that work in the section of the

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

service auditor's assurance report that contains the service auditor's opinion. (Ref: Para. A40)

37. In the case of a type 2 report, if the work of the internal audit function has been used in performing tests of controls, that part of the service auditor's assurance report that describes the service auditor's tests of controls and the results thereof shall include a description of the internal auditor's work and of the service auditor's procedures with respect to that work. (Ref: Para. A41)

Written Representations

38. The service auditor shall request the service organisation to provide written representations: (Ref: Para. A42)
- (a) That reaffirm the assertion accompanying the description of the system;
 - (b) That it has provided the service auditor with all relevant information and access agreed to;¹⁰ and
 - (c) That it has disclosed to the service auditor any of the following of which it is aware:
 - (i) Non-compliance with laws and regulations, fraud, or uncorrected deviations attributable to the service organisation that may affect one or more user entities;
 - (ii) Design deficiencies in controls;
 - (iii) Instances where controls have not operated as described; and
 - (iv) Any events subsequent to the period covered by the service organisation's description of its system up to the date of the service auditor's assurance report that could have a significant effect on the service auditor's assurance report.
39. The written representations shall be in the form of a representation letter addressed to the service auditor.¹¹ The date of the written

¹⁰ See paragraph 13(b)(vi) of this standard.

¹¹ An example representation letter is included in [Aus] Appendix 0B.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

representations shall be as near as practicable to, but not after, the date of the service auditor's assurance report.

40. If, having discussed the matter with the service auditor, the service organisation does not provide one or more of the written representations requested in accordance with paragraph 38(a) and (b) of this standard, the service auditor shall disclaim an opinion. (Ref: Para. A43)

Other Information

41. The service auditor shall read the other information, if any, included in a document containing the service organisation's description of its system and the service auditor's assurance report, 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 in that other information.
42. If the service auditor becomes aware of a material inconsistency or an apparent misstatement of fact in the other information, the service auditor shall discuss the matter with the service organisation. If the service auditor concludes that there is a material inconsistency or a misstatement of fact in the other information that the service organisation refuses to correct, the service auditor shall take further appropriate action. (Ref: Para. A44-A45)

Subsequent Events

43. The service auditor shall enquire whether the service organisation is aware of any events subsequent to the period covered by the service organisation's description of its system up to the date of the service auditor's assurance report that could have a significant effect on the service auditor's assurance report. If the service auditor is aware of such an event, and information about that event is not disclosed by the service organisation, the service auditor shall disclose it in the service auditor's assurance report.
44. The service auditor has no obligation to perform any procedures regarding the description of the service organisation's system, or the suitability of design or operating effectiveness of controls, after the date of the service auditor's assurance report.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Documentation

45. The service auditor shall prepare documentation that is sufficient 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 standard and applicable legal and regulatory requirements;
 - (b) The results of the procedures performed, and the evidence obtained; and
 - (c) Significant matters arising during the engagement, and the conclusions reached thereon and significant professional judgements made in reaching those conclusions.
46. 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 work and the date such work was completed; and
 - (c) Who reviewed the work performed and the date and extent of such review.
47. If the service auditor uses specific work of the internal auditors, the service auditor shall document the conclusions reached regarding the evaluation of the adequacy of the work of the internal auditors, and the procedures performed by the service auditor on that work.
48. The service auditor shall document discussions of significant matters with the service organisation and others including the nature of the significant matters discussed and when and with whom the discussions took place.
49. 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.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

50. The service auditor shall assemble the documentation in an engagement file and complete the administrative process of assembling the final engagement file on a timely basis after the date of the service auditor's assurance report.¹²
51. After the assembly of the final engagement file has been completed, the service auditor shall not delete or discard documentation before the end of its retention period. (Ref: Para. A46)
52. 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 and that documentation does not affect the service auditor's report, the service auditor shall, regardless of the nature of the modifications or additions, document:
- (a) The specific reasons for making them; and
 - (b) When and by whom they were made and reviewed.

Preparing the Service Auditor's Assurance Report

Content of the Service Auditor's Assurance Report

53. The service auditor's assurance report shall include the following basic elements: (Ref: Para. A47)
- (a) A title that clearly indicates the report is an independent service auditor's assurance report.
 - (b) An addressee.
 - (c) Identification of:
 - (i) The service organisation's description of its system, and the service organisation's assertion, which includes the matters described in paragraph 9(k)(ii) of this standard for a type 2 report, or paragraph 9(j)(ii) of this standard for a type 1 report.
 - (ii) Those parts of the service organisation's description of its system, if any, that are not covered by the service auditor's opinion.

¹² See Auditing Standard ASQC 1, paragraphs 45 and A54-A55.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (iii) If the description refers to the need for complementary user entity controls, a statement that the service auditor has not evaluated the suitability of design or operating effectiveness of complementary user entity controls, and that the control objectives stated in the service organisation's description of its system can be achieved only if complementary user entity controls are suitably designed or operating effectively, along with the controls at the service organisation.
- (iv) If services are performed by a subservice organisation, the nature of activities performed by the subservice organisation as described in the service organisation's description of its system and whether the inclusive method or the carve-out method has been used in relation to them. Where the carve-out method has been used, a statement that the service organisation's description of its system excludes the control objectives and related controls at relevant subservice organisations, and that the service auditor's procedures do not extend to controls at the subservice organisation. Where the inclusive method has been used, a statement that the service organisation's description of its system includes control objectives and related controls at the subservice organisation, and that the service auditor's procedures extended to controls at the subservice organisation.
- (d) Identification of the criteria, and the party specifying the control objectives.
- (e) A statement that the report and, in the case of a type 2 report, the description of tests of controls are intended only for user entities and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by user entities themselves, when assessing the risks of material misstatements of user entities' financial reports/statements. (Ref: Para. A48)
- (f) A statement that the service organisation is responsible for:

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (i) Preparing the description of its system, and the accompanying assertion, including the completeness, accuracy and method of presentation of that description and that assertion;
 - (ii) Providing the services covered by the service organisation's description of its system;
 - (iii) Stating the control objectives (where not identified by law or regulation, or another party, for example, a user group or a professional body); and
 - (iv) Designing and implementing controls to achieve the control objectives stated in the service organisation's description of its system.
- (g) A statement that the service auditor's responsibility is to express an opinion on the service organisation's description, on the design of controls related to the control objectives stated in that description and, in the case of a type 2 report, on the operating effectiveness of those controls, based on the service auditor's procedures.
- (h) A statement that the engagement was performed in accordance with ASAE 3402 *Assurance Reports on Controls at a Service Organisation*, which requires that the service auditor comply with ethical requirements and plan and perform procedures to obtain reasonable assurance about whether, in all material respects, the service organisation's description of its system is fairly presented and the controls are suitably designed and, in the case of a type 2 report, are operating effectively.
- (i) A summary of the service auditor's procedures to obtain reasonable assurance and a statement of the service auditor's belief that the evidence obtained is sufficient and appropriate to provide a basis for the service auditor's opinion, and, in the case of a type 1 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.
- (j) A statement of the limitations of controls and, in the case of a type 2 report, of the risk of projecting to future periods any evaluation of the operating effectiveness of controls.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (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 2 report:
 - a. The description fairly presents the service organisation's system that had been designed and implemented throughout the specified period;
 - b. The controls related to the control objectives stated in the service organisation's description of its system were suitably designed throughout the specified period; and
 - c. The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the specified period.
 - (ii) In the case of a type 1 report:
 - a. The description fairly presents the service organisation's system that had been designed and implemented as at the specified date; and
 - b. The controls related to the control objectives stated in the service organisation's description of its system were suitably designed as at the specified date.
- (l) The date of the service auditor's assurance report, which shall be no earlier than the date on which the service auditor has obtained sufficient appropriate evidence on which to base the opinion.
- (m) The name of the service auditor, and the location in the jurisdiction where the service auditor practices.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

54. In the case of a type 2 report, the service auditor's assurance report shall include a separate section after the opinion, or an attachment, that describes the tests of controls that were performed and the results of those tests. In describing the tests of controls, the service auditor shall clearly state which controls were tested, identify whether the items tested represent all or a selection of the items in the population, and indicate the nature of the tests in sufficient detail to enable user auditors to determine the effect of such tests on their risk assessments. If deviations have been identified, the service auditor shall include the extent of testing performed that led to identification of the deviations (including the sample size where sampling has been used), and the number and nature of the deviations 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 was achieved. (Ref: Para. A18 and A49)

Modified Opinions

55. If the service auditor concludes that: (Ref: Para. A50-A52)
- (a) The service organisation's description does not fairly present, in all material respects, the system as designed and implemented;
 - (b) The controls related to the control objectives stated in the description were not suitably designed, in all material respects;
 - (c) In the case of a type 2 report, the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the service organisation's description of its system were achieved, did not operate effectively, in all material respects; 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.

Other Communication Responsibilities

56. If the service auditor becomes aware of non-compliance with laws and regulations, fraud, or uncorrected errors attributable to the

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

service organisation that are not clearly trivial and may affect one or more user entities, the service auditor shall determine whether the matter has been communicated appropriately to affected user entities. If the matter has not been so communicated and the service organisation is unwilling to do so, the service auditor shall take appropriate action. (Ref: Para. A53)

* * *

Draft

Application and Other Explanatory Material

Scope of this Standard on Assurance Engagements (Ref: Para. 1 and 3)

- A1. Internal control is a process designed to provide reasonable assurance regarding the achievement of objectives related to the reliability of financial reporting, effectiveness and efficiency of operations and compliance with applicable laws and regulations. Controls related to a service organisation's operations and compliance objectives may be relevant to a user entities' internal control as it relates to financial reporting. Such controls may pertain to assertions about presentation and disclosure relating to account balances, classes of transactions or disclosures, or may pertain to evidence that the user auditor evaluates or uses in applying auditing procedures. For example, a payroll processing service organisation's controls related to the timely remittance of payroll deductions to government authorities may be relevant to a user entity as late remittances could incur interest and penalties that would result in a liability for the user entity. Similarly, a service organisation's controls over the acceptability of investment transactions from a regulatory perspective may be considered relevant to a user entity's presentation and disclosure of transactions and account balances in its financial report/statements. The determination of whether controls at a service organisation related to operations and compliance are likely to be relevant to user entities' internal control as it relates to financial reporting is a matter of professional judgement, having regard to the control objectives set by the service organisation and the suitability of the criteria.
- A2. The service organisation may not be able to assert that the system is suitably designed when, for example, the service organisation is operating a system that has been designed by a user entity or is stipulated in a contract between a user entity and the service organisation. Because of the inextricable link between the suitable design of controls and their operating effectiveness, the absence of an assertion with respect to the suitability of design will likely preclude the service auditor from concluding that the controls provide reasonable assurance that the control objectives have been met and thus from opining on the operating effectiveness of controls. As an alternative, the practitioner may choose to accept an agreed-upon procedures engagement to perform tests of controls, or an assurance engagement under ASAE 3000 to conclude on whether, based on tests of controls, the controls have operated as described.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Definitions (Ref: Para. 9(d) and 9(g))

- A3. The definition of “controls at the service organisation” includes aspects of user entities’ information systems maintained by the service organisation, and may also include aspects of one or more of the other components of internal control at a service organisation. For example, it may include aspects of a service organisation’s control environment, monitoring, and control activities when they relate to the services provided. It does not, however, include controls at a service organisation that are not related to the achievement of the control objectives stated in the service organisation’s description of its system, for example, controls related to the preparation of the service organisation’s own financial report/statements.
- A4. When the inclusive method is used, the requirements in this standard also apply to the services provided by the subservice organisation, including obtaining agreement regarding the matters in paragraph 13(b)(i)-(vi) as applied to the subservice organisation rather than the service organisation. Performing procedures at the subservice organisation entails coordination and communication between the service organisation, the subservice organisation, and the service auditor. The inclusive method generally is feasible only if the service organisation and the subservice organisation are related, or if the contract between the service organisation and the subservice organisation provides for its use.

Ethical Requirements (Ref: Para. 11)

- A5. [Deleted by the AUASB. Refer Aus A5.1].
- Aus A5.1 The service auditor is subject to relevant independence requirements, which comprise the requirements referenced in ASA 102 *Compliance with Ethical Requirements when Performing Audits, Reviews and Other Assurance Engagements*. In performing an engagement in accordance with this standard, relevant independence requirements do not require the service auditor to be independent from each user entity.

Management and Those Charged with Governance (Ref: Para. 12)

- A6. Management and governance structures vary by jurisdiction and by entity, reflecting influences such as different cultural and legal backgrounds, and size and ownership characteristics. Such diversity

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

means that it is not possible for this standard to specify for all engagements the person(s) with whom the service auditor is to interact regarding particular matters. For example, the service organisation may be a segment of a third-party organisation and not a separate legal entity. In such cases, identifying the appropriate management personnel or those charged with governance from whom to request written representations may require the exercise of professional judgement.

Acceptance and Continuance

Capabilities and Competence to Perform the Engagement (Ref: Para. 13(a)(i))

- A7. Relevant capabilities and competence to perform the engagement include matters such as the following:
- Knowledge of the relevant industry;
 - An understanding of information technology and systems;
 - Experience in evaluating risks as they relate to the suitable design of controls; and
 - Experience in the design and execution of tests of controls and the evaluation of the results.

Service Organisation's Assertion (Ref: Para. 13(b)(i))

- A8. Refusal, by a service organisation, to provide a written assertion, subsequent to an agreement by the service auditor to accept, or continue, an engagement, represents a scope limitation that causes the service auditor to withdraw from the engagement. If law or regulation does not allow the service auditor to withdraw from the engagement, the service auditor disclaims an opinion.

Reasonable Basis for Service Organisation's Assertion (Ref: Para. 13(b)(ii))

- A9. In the case of a type 2 report, the service organisation's assertion includes a statement that the controls related to the control objectives stated in the service organisation's description of its system operated effectively throughout the specified period. This assertion may be based on the service organisation's monitoring activities. Monitoring of controls is a process to assess the effectiveness of controls over time. It involves assessing the effectiveness of controls on a timely basis, identifying and reporting

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

deficiencies to appropriate individuals within the service organisation, and taking necessary corrective actions. The service organisation accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of both. The greater the degree and effectiveness of ongoing monitoring activities, the less need for separate evaluations. Ongoing monitoring activities are often built into the normal recurring activities of a service organisation and include regular management and supervisory activities. Internal auditors or personnel performing similar functions may contribute to the monitoring of a service organisation's activities. Monitoring activities may also include using information communicated by external parties, such as customer complaints and regulator comments, which may indicate problems or highlight areas in need of improvement. The fact that the service auditor will report on the operating effectiveness of controls is not a substitute for the service organisation's own processes to provide a reasonable basis for its assertion.

Identification of Risks (Ref: Para. 13(b)(v))

- A10. As noted in paragraph 9(c), control objectives relate to risks that controls seek to mitigate. For example, the risk that a transaction is recorded at the wrong amount or in the wrong period can be expressed as a control objective that transactions are recorded at the correct amount and in the correct period. The service organisation is responsible for identifying the risks that threaten achievement of the control objectives stated in the description of its system. The service organisation may have a formal or informal process for identifying relevant risks. A formal process may include estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, since control objectives relate to risks that controls seek to mitigate, thoughtful identification of control objectives when designing and implementing the service organisation's system may itself comprise an informal process for identifying relevant risks.

Acceptance of a Change in the Terms of the Engagement (Ref: Para. 14)

- A11. A request to change the scope of the engagement may not have a reasonable justification when, for example, the request is made to exclude certain control objectives from the scope of the engagement because of the likelihood that the service auditor's opinion would be modified; or the service organisation will not provide the service auditor with a written assertion and the request is made to perform the engagement under ASAE 3000.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

A12. A request to change the scope of the engagement may have a reasonable justification when, for example, the request is made to exclude from the engagement a subservice organisation when the service organisation cannot arrange for access by the service auditor, and the method used for dealing with the services provided by that subservice organisation is changed from the inclusive method to the carve-out method.

Aus A12.1 An example engagement letter is contained in [Aus] Appendix 0A.

Assessing the Suitability of the Criteria (Ref: Para. 15-18)

A13. Criteria need to be available to the intended users to allow them to understand the basis for the service organisation's assertion about the fair presentation of its description of the system, the suitability of the design of controls and, in the case of a type 2 report, the operating effectiveness of the controls related to the control objectives.

A14. ASAE 3000 requires the service auditor, among other things, to assess the suitability of criteria, and the appropriateness of the subject matter.¹³ The subject matter is the underlying condition of interest to intended users of an assurance report. The following table identifies the subject matter and minimum criteria for each of the opinions in type 2 and type 1 reports.

¹³ ASAE 3000, paragraphs 33-39.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

	Subject matter	Criteria	Comment
	<p>The service organisation's system that is likely to be relevant to user entities' internal control as it relates to financial reporting and is covered by the service auditor's assurance report.</p>	<p>The description is fairly presented if it: (a) presents how the service organisation's system was designed and implemented including, as appropriate, the matters identified in paragraph 16(a)(i)-(viii); (b) in the case of a type 2 report, includes relevant details of changes to the service organisation's system during the period covered by the description; and (c) does not omit or distort information relevant to the scope of the service organisation's system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and may not, therefore, include every aspect of the service organisation's system that each individual user entity may consider important in its own particular environment.</p>	<p>The specific wording of the criteria for this opinion may need to be tailored to be consistent with criteria established by, for example, law or regulation, user groups, or a professional body. Examples of criteria for this opinion are provided in the illustrative service organisation's assertion in Appendix 1. Paragraphs A21-A24 offer further guidance on determining whether these criteria are met. (In terms of the requirements of ASAE 3000, the subject matter information¹⁴ for this opinion is the service organisation's description of its system and the service organisation's assertion that the description is fairly presented.)</p>

¹⁴ 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.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

	Subject matter	Criteria	Comment	
<i>Opinion about suitability of design, and operating effectiveness (type 2 reports)</i>	The suitability of the design and operating effectiveness of those controls that are necessary to achieve the control objectives stated in the service organisation's description of its system.	The controls are suitably designed and operating effectively if: (a) the service organisation has identified the risks that threaten achievement of the control objectives stated in the description of its system; (b) the controls identified in that description would, if operated as described, provide reasonable assurance that those risks do not prevent the stated control objectives from being achieved; and (c) the controls were consistently applied as designed throughout the specified period. This includes whether manual controls were applied by individuals who have the appropriate competence and authority.	When 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 ASAE 3000, the subject matter information for this opinion is the service organisation's assertion that controls are suitably designed and that they are operating effectively.)	The control objectives, which are stated in the service organisation's description of its system, are part of the criteria for these opinions. The stated control objectives will differ from engagement to engagement. If, as part of forming the opinion on the description, the service auditor concludes the stated control objectives are not fairly presented then those control objectives would not be suitable as part of the criteria for forming an opinion on either the design or operating effectiveness of controls.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

	Subject matter	Criteria	Comment	
<i>Opinion about suitability of design (type 1 reports)</i>	The suitability of the design of those controls that are necessary to achieve the control objectives stated in the service organisation's description of its system.	The controls are suitably designed if: (a) the service organisation has identified the risks that threaten achievement of the control objectives stated in the description of its system; and (b) the controls identified in that description would, if operated as described, provide reasonable assurance that those risks do not prevent the stated control objectives from being achieved.	Meeting these criteria 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 ASAE 3000, the subject matter information for this opinion is the service organisation's assertion that controls are suitably designed.)	The control objectives, which are stated in the service organisation's description of its system, are part of the criteria for these opinions. The stated control objectives will differ from engagement to engagement. If, as part of forming the opinion on the description, the service auditor concludes the stated control objectives are not fairly presented then those control objectives would not be suitable as part of the criteria for forming an opinion on the design.

A15. Paragraph 16(a) identifies a number of elements that are included in the service organisation's description of its system as appropriate. These elements may not be appropriate if the system being described is not a system that processes transactions, for example, if the system relates to general controls over the hosting of an IT application but not the controls embedded in the application itself.

Materiality (Ref: Para. 19 and 54)

A16. In an engagement to report on controls at a service organisation, the concept of materiality relates to the system being reported on, not the financial reports/statements of user entities. The service auditor plans

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

and performs procedures to determine whether the service organisation's description of its system is fairly presented in all material respects, whether controls at the service organisation are suitably designed in all material respects and, in the case of a type 2 report, whether controls at the service organisation are operating effectively in all material respects. The concept of materiality takes into account that the service auditor's assurance report provides information about the service organisation's system to meet the common information needs of a broad range of user entities and their auditors who have an understanding of the manner in which that system has been used.

- A17. Materiality with respect to the fair presentation of the service organisation's description of its system, and with respect to the design of controls, includes primarily the consideration of qualitative factors, for example: whether the description includes the significant aspects of processing significant transactions; whether the description omits or distorts relevant information; and the ability of controls, as designed, to provide reasonable assurance that control objectives would be achieved. Materiality with respect to the service auditor's opinion on the operating effectiveness of controls includes the consideration of both quantitative and qualitative factors, for example, the tolerable rate and observed rate of deviation (a quantitative matter), and the nature and cause of any observed deviation (a qualitative matter).
- A18. The concept of materiality is not applied when disclosing, in the description of the tests of controls, the results of those tests where deviations have been identified. This is because, in the particular circumstances of a specific user entity or user auditor, a deviation may have significance beyond whether or not, in the opinion of the service auditor, it prevents a control from operating effectively. For example, the control to which the deviation relates may be particularly significant in preventing a certain type of error that may be material in the particular circumstances of a user entity's financial report/statements.

Obtaining an Understanding of the Service Organisation's System

(Ref: Para. 20)

- A19. Obtaining an understanding of the service organisation's system, including controls, included in the scope of the engagement, assists the service auditor in:
- Identifying the boundaries of that system, and how it interfaces with other systems.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- Assessing whether the service organisation's description fairly presents the system that has been designed and implemented.
 - Determining which controls are necessary to achieve the control objectives stated in the service organisation's description of its system.
 - Assessing whether controls were suitably designed.
 - Assessing, in the case of a type 2 report, whether controls were operating effectively.
- A20. The service auditor's procedures to obtain this understanding may include:
- Enquiring of those within the service organisation who, in the service auditor's judgement, may have relevant information.
 - Observing operations and inspecting documents, reports, printed and electronic records of transaction processing.
 - Inspecting a selection of agreements between the service organisation and user entities to identify their common terms.
 - Reperforming control procedures.

Obtaining Evidence Regarding the Description (Ref: Para. 21-22)

- A21. Considering the following questions may assist the service auditor in determining whether those aspects of the description included in the scope of the engagement are fairly presented in all material respects:
- Does the description address the major aspects of the service provided (within the scope of the engagement) that could reasonably be expected to be relevant to the common needs of a broad range of user auditors in planning their audits of user entities' financial reports/statements?
 - Is the description prepared at a level of detail that could reasonably be expected to provide a broad range of user auditors with sufficient information to obtain an understanding of internal control in accordance with

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

ASA 315?¹⁵ The description need not address every aspect of the service organisation'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 at the service organisation.

- Is the description prepared in a manner that does not omit or distort information that may affect the common needs of a broad range of user auditors' decisions, for example, does the description contain any significant omissions or inaccuracies in processing of which the service auditor is aware?
- Where some of the control objectives stated in the service organisation's description of its system have been excluded from the scope of the engagement, does the description clearly identify the excluded objectives?
- Have the controls identified in the description been implemented?
- Are complementary user entity controls, if any, described adequately? 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 organisation alone. In some cases, however, the control objectives stated in the service organisation's description of its system cannot be achieved by the service organisation alone because their achievement requires particular controls to be implemented by user entities. This may be the case where, for example, the control objectives are specified by a regulatory authority. When the description does include complementary user entity controls, the description separately identifies those controls along with the specific control objectives that cannot be achieved by the service organisation alone.
- If the inclusive method has been used, does the description separately identify controls at the service organisation and controls at the subservice organisation? If the carve-out method is used, does the description identify the functions that are performed by the subservice organisation? When the carve-out method is used, the description need not describe

¹⁵ See ASA 315 *Identifying and Assessing Risks of Material Misstatement through Understanding the Entity and Its Environment*.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

the detailed processing or controls at the subservice organisation.

A22. The service auditor's procedures to evaluate the fair presentation of the description may include:

- Considering the nature of user entities and how the services provided by the service organisation are likely to affect them, for example, whether user entities are from a particular industry and whether they are regulated by government agencies.
- Reading standard contracts, or standard terms of contracts, (if applicable) with user entities to gain an understanding of the service organisation's contractual obligations.
- Observing procedures performed by service organisation personnel.
- Reviewing the service organisation's policy and procedure manuals and other systems documentation, for example, flowcharts and narratives.

A23. Paragraph 21(a) requires the service auditor to evaluate whether the control objectives stated in the service organisation's description of its system are reasonable in the circumstances. Considering the following questions may assist the service auditor in this evaluation:

- Have the stated control objectives been designated by the service organisation or by outside parties such as a regulatory authority, a user group, or a professional body that follows a transparent due process?
- Where the stated control objectives have been specified by the service organisation, do they relate to the types of assertions commonly embodied in the broad range of user entities' financial reports/statements to which controls at the service organisation could reasonably be expected to relate? Although the service auditor ordinarily will not be able to determine how controls at a service organisation specifically relate to the assertions embodied in individual user entities' financial reports/statements, the service auditor's understanding of the nature of the service organisation's system, including controls, and services being provided is

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

used to identify the types of assertions to which those controls are likely to relate.

- Where the stated control objectives have been specified by the service organisation, are they complete? A complete set of control objectives can provide a broad range of user auditors with a framework to assess the effect of controls at the service organisation on the assertions commonly embodied in user entities' financial reports/statements.

A24. The service auditor's procedures to determine whether the service organisation's system has been implemented may be similar to, and performed in conjunction with, procedures to obtain an understanding of that system. They may also include tracing items through the service organisation's system and, in the case of a type 2 report, specific enquiries about changes in controls that were implemented during the period. Changes that are significant to user entities or their auditors are included in the description of the service organisation's system.

Obtaining Evidence Regarding Design of Controls (Ref: Para. 23 and 28(b))

A25. From the viewpoint of a user entity or 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 organisation or a service auditor, however, is not aware of the circumstances at individual user entities that would determine whether or not a misstatement resulting from a control deviation is material to those user entities. 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 control objectives stated in the service organisation's description of its system are achieved.

A26. A service auditor may consider using flowcharts, questionnaires, or decision tables to facilitate understanding the design of the controls.

A27. Controls may consist of a number of activities directed at the achievement of a control objective. Consequently, if the service auditor evaluates certain activities as being ineffective in achieving a particular control objective, the existence of other activities may allow the service auditor to conclude that controls related to the control objective are suitably designed.

Obtaining Evidence Regarding Operating Effectiveness of Controls

Assessing Operating Effectiveness (Ref: Para. 24)

- A28. From the viewpoint of a user entity or a user auditor, a control is operating effectively if, individually or in combination with other controls, it provides reasonable assurance that material misstatements, whether due to fraud or error, are prevented, or detected and corrected. A service organisation or a service auditor, however, is not aware of the circumstances at individual user entities that would determine whether a misstatement resulting from a control deviation had occurred and, if so, whether it 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 control objectives stated in the service organisation's description of its system are achieved. Similarly, a service organisation or a service auditor is not in a position to determine whether any observed control deviation would result in a material misstatement from the viewpoint of an individual user entity.
- A29. Obtaining an understanding of controls sufficient to opine on the suitability of their design 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 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 service auditor's assessment and testing of other controls, such as those over program changes.
- A30. To be useful to user auditors, a type 2 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 result in 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 organisation (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

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

before issuing a report or to issue a report covering the system both before and after the changes.

- A31. 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 necessary to test the operating effectiveness of such control procedures at various times throughout the reporting period.
- A32. The service auditor provides an opinion on the operating effectiveness of controls throughout each period, therefore, sufficient appropriate evidence about the operation of controls during the current period is required for the service auditor to express that opinion. Knowledge of deviations observed in prior engagements may, however, lead the service auditor to increase the extent of testing during the current period.

Testing of Indirect Controls (Ref: Para. 25(b))

- A33. In some circumstances, it may be necessary to obtain evidence supporting the effective operation of indirect controls. For example, when the service auditor decides to test the effectiveness of a review of exception reports detailing sales in excess of authorised credit limits, the review and related follow up is the control that is directly of relevance to the service auditor. Controls over the accuracy of the information in the reports (for example, the general IT controls) are described as “indirect” controls.
- A34. Because of the inherent consistency of IT processing, evidence about the implementation of an automated application control, when considered in combination with evidence about the operating effectiveness of the service organisation’s general controls (in particular, change controls), may also provide substantial evidence about its operating effectiveness.

Means of Selecting Items for Testing (Ref: Para. 25(c) and 27)

- A35. The means of selecting items for testing available to the service auditor are:
- (a) Selecting all items (100% examination). This may be appropriate for testing controls that are applied infrequently, for example, quarterly, or when evidence regarding application of the control makes 100% examination efficient;

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (b) Selecting specific items. This may be appropriate where 100% examination would not be efficient and sampling would not be effective, such as testing controls that are not applied sufficiently frequently to render a large population for sampling, for example, controls that are applied monthly or weekly; and
- (c) Sampling. This may be appropriate for testing controls that are applied frequently in a uniform manner and which leave documentary evidence of their application.
- A36. While selective examination of specific items will often be an efficient means of obtaining evidence, it does not constitute sampling. The results of procedures applied to items selected in this way cannot be projected to the entire population; accordingly, selective examination of specific items does not provide evidence concerning the remainder of the population. Sampling, on the other hand, is designed to enable conclusions to be drawn about an entire population on the basis of testing a sample drawn from it.

The Work of an Internal Audit Function

Obtaining an Understanding of the Internal Audit Function (Ref: Para. 30)

- A37. An internal audit function may be responsible for providing analyses, evaluations, assurances, recommendations, and other information to management and those charged with governance. An internal audit function at a service organisation may perform activities related to the service organisation's own system of internal control, or activities related to the services and systems, including controls, that the service organisation is providing to user entities.

Determining Whether and to What Extent to Use the Work of the Internal Auditors (Ref: Para. 33)

- A38. In determining the planned effect of the work of the internal auditors on the nature, timing or extent of the service auditor's procedures, the following factors may suggest the need for different or less extensive procedures than would otherwise be the case:
- The nature and scope of specific work performed, or to be performed, by the internal auditors is quite limited.
 - The work of the internal auditors relates to controls that are less significant to the service auditor's conclusions.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- The work performed, or to be performed, by the internal auditors does not require subjective or complex judgements.

Using the Work of the Internal Audit Function (Ref: Para. 34)

A39. The nature, timing and extent of the service auditor's procedures on specific work of the internal auditors will depend on the service auditor's assessment of the significance of that work to the service auditor's conclusions (for example, the significance of the risks that the controls tested seek to mitigate), the evaluation of the internal audit function and the evaluation of the specific work of the internal auditors. Such procedures may include:

- Examination of items already examined by the internal auditors;
- Examination of other similar items; and
- Observation of procedures performed by the internal auditors.

Effect on the Service Auditor's Assurance Report (Ref: Para. 36-37)

A40. Irrespective of the degree of autonomy and objectivity of the internal audit function, such function is not independent of the service organisation as is required of the service auditor when performing the engagement. The service auditor has sole responsibility for the opinion expressed in the service auditor's assurance report, and that responsibility is not reduced by the service auditor's use of the work of the internal auditors.

A41. The service auditor's description of work performed by the internal audit function may be presented in a number of ways, for example:

- By including introductory material to the description of tests of controls indicating that certain work of the internal audit function was used in performing tests of controls.
- Attribution of individual tests to internal audit.

Written Representations (Ref: Para. 38 and 40)

A42. The written representations required by paragraph 38 are separate from, and in addition to, the service organisation's assertion, as defined at paragraph 9(o).

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

A43. If the service organisation does not provide the written representations requested in accordance with paragraph 38(c) of this standard, it may be appropriate for the service auditor's opinion to be modified in accordance with paragraph 55(d) of this standard.

Other Information (Ref: Para. 42)

A44. Relevant ethical requirements require that a service auditor not be associated with information where the service auditor believes that the information:

- (a) Contains a materially false or misleading statement;
- (b) Contains statements or information furnished recklessly; or
- (c) Omits or obscures information required to be included where such omission or obscurity would be misleading.¹⁶

If other information included in a document containing the service organisation's description of its system and the service auditor's assurance report contains future-oriented information such as recovery or contingency plans, or plans for modifications to the system that will address deviations identified in the service auditor's assurance report, or claims of a promotional nature that cannot be reasonably substantiated, the service auditor may request that information be removed or restated.

A45. If the service organisation refuses to remove or restate the other information, further actions that may be appropriate include, for example:

- Requesting the service organisation to consult with its legal counsel as to the appropriate course of action.
- Describing the material inconsistency or material misstatement of fact in the assurance report.
- Withholding the assurance report until the matter is resolved.
- Withdrawing from the engagement.

¹⁶ See ASA 102.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Documentation (Ref: Para. 51)

- A46. ASQC 1 requires firms to establish policies and procedures for the timely completion of the assembly of engagement files.¹⁷ An appropriate time limit within which to complete the assembly of the final engagement file is ordinarily not more than 60 days after the date of the service auditor's report.¹⁸

Preparing the Service Auditor's Assurance Report

Content of the Service Auditor's Assurance Report (Ref: Para. 53)

- A47. Illustrative examples of service auditors' assurance reports, related service organisations' assertions and a description of the system are contained in Appendices 1, [Aus] 1A and 2.

Intended Users and Purposes of the Service Auditor's Assurance Report
(Ref: Para. 53(e))

- A48. The criteria used for engagements to report on controls at a service organisation are relevant only for the purposes of providing information about the service organisation's system, including controls, to those who have an understanding of how the system has been used for financial reporting by user entities. Accordingly this is stated in the service auditor's assurance report. In addition, the service auditor may consider it appropriate to include wording that specifically restricts distribution of the assurance report other than to intended users, its use by others, or its use for other purposes.

Description of the Tests of Controls (Ref: Para. 54)

- A49. In describing the nature of the tests of controls for a type 2 report, it assists readers of the service auditor's assurance report if the service auditor includes:
- The results of all tests where deviations have been identified, even if other controls have been identified that allow the service auditor to conclude that the relevant control objective has been achieved or the control tested has subsequently been removed from the service organisation's description of its system.

¹⁷

See ASQC 1, paragraph 45.

¹⁸

See ASQC 1, paragraph A54.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- Information about causative factors for identified deviations, to the extent the service auditor has identified such factors.

Modified Opinions (Ref: Para. 55)

- A50. Illustrative examples of elements of modified service auditor's assurance reports are contained in Appendix 3.
- A51. Even if the service auditor has expressed an adverse opinion or disclaimed an opinion, it may be appropriate to describe in the basis for modification paragraph the reasons for any other matters of which the service auditor is aware that would have required a modification to the opinion, and the effects thereof.
- A52. When expressing a disclaimer of opinion because of a scope limitation, it is not ordinarily appropriate to identify the procedures that were performed nor include statements describing the characteristics of a service auditor's engagement; to do so might overshadow the disclaimer of opinion.

Other Communication Responsibilities (Ref: Para. 56)

- A53. Appropriate actions to respond to the circumstances identified in paragraph 56 may include:
- Obtaining legal advice about the consequences of different courses of action.
 - Communicating with those charged with governance of the service organisation.
 - Communicating with third parties (for example, a regulator) when required to do so.
 - Modifying the service auditor's opinion, or adding an Other Matter paragraph.
 - Withdrawing from the engagement.

Conformity with International Standards on Assurance Engagements

This Standard on Assurance Engagements conforms with International Standard on Assurance Engagements ISAE 3402 *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board (IAASB), an independent standard-setting board of the International Federation of Accountants (IFAC).

Paragraphs that have been added to this Standard on Assurance Engagements (and do not appear in the text of the equivalent ISAE) are identified with the prefix “Aus”.

The following requirements are additional to ISAE 3402:

- The standard does not deal with instances when individual internal auditors provide direct assistance to the service auditor in carrying out assurance procedures. (Ref: Para. Aus 30.1)

Appendices containing guidance which have been added to this Standard on Assurance Engagements (and do not appear in the appendices of the equivalent ISAE) are identified with the prefix “Aus”.

The following appendices are additional to ISAE 3402:

- [Aus] Appendix 0A *Example Engagement Letter*
- [Aus] Appendix 0B *Example Representation Letter*
- [Aus] Appendix 1A: *Illustrative Example of a Service Organisation’s Description of the System Accompanying XYZ Service Organisation Management’s Assertion*

Compliance with this Standard enables compliance with ISAE 3402 .

[Aus] Appendix 0A

(Ref: Para. Aus A12.1)

Example Engagement Letter

The following example of a service auditor's engagement letter is for guidance only and is not intended to be exhaustive or applicable to all situations.

Service Auditor's Engagement Letter for a Type 2 Report

To [the appropriate representative of management or those charged with governance] of XYZ Service Organisation:

[The objective and scope of the engagement]

You have requested that we report on the description of XYZ Service Organisation's [the type or name of] system and management's assertion with respect to that description, which you will provide and which will accompany our report. The description of XYZ Service Organisation's [the type or name of] system comprises control objectives which are likely to be relevant to customers', who have used [the type or name of system], internal control as it relates to financial reporting and related controls designed to achieve those objectives for the [period] ended [date]. We are pleased to confirm our acceptance and our understanding of this assurance engagement by means of this letter. Our assurance engagement will be conducted with the objective of our expressing an opinion on the fair presentation of the [the type or name of] system, suitability of the design of the controls to achieve the control objectives throughout the period and the operating effectiveness of the controls necessary to provide reasonable assurance that the control objectives were achieved throughout the period.

[Responsibilities of the assurance practitioner]

We will conduct our assurance engagement in accordance with Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation*. That standard requires that we comply with ethical requirements and plan and perform procedures to obtain reasonable assurance about whether, in all material respects, XYZ Service Organisation's description of the [the type or name of] system is fairly presented, the controls are suitably designed and operating effectively. An assurance engagement involves performing procedures to obtain evidence about the description, design and operating effectiveness of controls. The procedures selected depend on the assurance practitioner's judgement, including the

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

assessment of the risks of significant deficiencies in the [the type or name of] system.

Because of the inherent limitations of an assurance engagement, together with the inherent limitations of any internal control system there is an unavoidable risk that some significant deficiencies may not be detected, even though the engagement is properly planned and performed in accordance with Standards on Assurance Engagements.

Further, the system, within which the controls operate that we will test, will not be examined except to the extent the [the type or name of] system, is likely to be relevant to customers', who have used [the type or name of] system, internal control as it relates to financial reporting. Hence no opinion will be expressed as to the effectiveness of the internal control system as a whole.

The work undertaken by us to form an opinion is permeated by judgement, in particular regarding the nature timing and extent of assurance procedures for gathering evidence and the drawing of conclusions based on the evidence gathered. In addition to the inherent limitations in any assurance engagement, which include the use of testing, inherent limitations of any internal control structure, and the possibility of collusion, most evidence is persuasive rather than conclusive. As a result, an assurance engagement can only provide reasonable – not absolute – assurance that the description is fairly presented, controls are suitably designed and controls have operated effectively throughout the period.

[The responsibilities of management and identification of the applicable control framework]

Our assurance engagement will be conducted on the basis that [management or, where appropriate, those charged with governance] acknowledge and understand that they have responsibility:

- (a) For the preparation of a written assertion that, in all material respects, and based on suitable criteria:
 - (i) the description fairly presents the XYZ Service Organisation's [the type or name of] system designed and implemented throughout the period;
 - (ii) The controls related to the control objectives stated in XYZ Service Organisation's description of its system were suitably designed throughout the specified period;

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (iii) The controls related to the control objectives stated in XYZ Service Organisation's description of its system operated effectively throughout the specified period.
- (b) For design of the system, comprising controls which will achieve control objectives which are likely to be relevant to customers', who have used [the type or name of] system, internal control as it relates to financial reporting;
- (c) To provide us with:
 - (i) Access to all information of which those charged with governance and management are aware that is relevant to the design, implementation and operation of the [the type or name of] system;
 - (ii) Additional information that we may request from those charged with governance and management for the purposes of this assurance engagement; and
 - (iii) Unrestricted access to persons within the entity from whom we determine it necessary to obtain evidence.

As part of our assurance process, we will request from [management and, where appropriate, those charged with governance], written confirmation concerning representations made to us in connection with the engagement.

[Assurance Approach]

We will examine and evaluate the control objectives and controls for [the type or name of] system described above. The "Description of [the type or name of] System" will include details of controls with which customers should comply. While our evaluation will include assessment of the appropriateness of the complementary customer controls, our testing will not encompass evaluation of the suitability of design or operating effectiveness of controls carried out by users of XYZ Service Organisation's [the type or name of] system. The control objectives stated in XYZ Service Organisation's description of its system can be achieved only if complementary user entity controls are suitably designed or operating effectively, along with the controls at the service organisation.

Our procedures will extend to the control objectives and related controls at relevant subservice organisations only to the extent that those controls are included in XYZ Service Organisation's description of [the type or name of] system and are necessary to achieve the relevant control objectives.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Due to the complex nature of internal control, our assurance procedures will not encompass all individual controls at XYZ Service Organisation, but will be restricted to an examination of those controls reported which achieve the control objectives identified by XYZ Service Organisation's management in the "Description of the [the type or name of] System" provided to us.

[Assurance Procedures]

Our assurance procedures are likely to include:

1. Performing a preliminary review of the control environment of XYZ Service Organisation relevant to the [the type or name of] system;
2. Evaluating the reasonableness of the control objectives;
3. Evaluating the completeness, accuracy and presentation of the Description of the [the type or name of] System against the controls implemented.
4. Evaluating the design of specific controls by:
 - Assessing the risks that threaten the achievement of the control objectives.
 - Evaluating whether the controls described are capable of addressing those risks and achieving the related objectives.
5. Performing tests of controls to ascertain whether the degree of compliance with controls is sufficient to provide reasonable assurance that the controls have achieved their objectives throughout the period.

In undertaking this engagement, we shall work closely with XYZ Service Organisation's internal audit function and place reliance on their work in accordance with ASA 610 *Using the Work of Internal Auditors* (paragraph applicable where the work of internal audit is an integral part of the assurance engagement).

[Assurance Report]

The format of the report will be in accordance with ASAE 3402 and will consist of an opinion on the "Description of the [the type or name of] system" by XYZ Service Organisation management and an accompanying description of the tests of controls that we performed and the results of those tests. An example of the proposed report is contained in the appendix to this letter.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Our report will be issued [frequency] and will cover [period reported on] (paragraph is appropriate for recurring engagements).

The assurance report will be incorporated in a report issued by the XYZ Service Organisation containing information prepared by XYZ Service Organisation management to provide customers and their auditors with an overall understanding of [subject matter]. We will review the contents of the report issued by XYZ Service Organisation to identify any material inconsistencies with the Description of the [the type or name of] System.

[Distribution of the Assurance Report]

Our report and the accompanying description of tests of controls are intended only for customers of XYZ Service Organisation which use the [the type or name of] system and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial reports.

The assurance report will be prepared for this purpose only and we disclaim any assumption of responsibility for any reliance on our report to any person other than to XYZ Service Organisation's customers and their auditors, or for any purpose other than that for which it was prepared.

[Significant Deficiencies in Controls]

We will issue an assurance report without modification, to provide assurance on the [the type or name of] system where our procedures do not disclose a significant deficiency in the controls necessary to achieve the control objectives contained in the Description of the [the type or name of] System by XYZ Service Organisation management. For this purpose, a significant deficiency exists when prescribed control procedures, or the degree of compliance with them:

- (a) does not provide XYZ Service Organisation management with reasonable assurance that the control objectives will be met or that fraud, error, or non-compliance with laws and regulations would be prevented or detected by employees in the normal course of their assigned functions; and
- (b) knowledge of that deficiency would be material to users of the assurance report.

If our assurance engagement discloses that there are significant deficiencies in the system of controls in operation during the period covered by the report,

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

such deficiencies will be disclosed in our report even if they were corrected prior to the end of the reporting period. However, our report will indicate that such deficiencies were corrected if that is the case. If any significant deficiencies disclosed in our report have been corrected subsequent to this period (or are in the process of being corrected), we will refer to this in our report.

Although the primary purpose of our assurance engagement will be to enable us to issue the above described report, we will also periodically provide you with letters containing recommendations for strengthening controls if such matters are observed during the process of the assurance engagement. Although issues raised may not represent significant deficiencies in the system of controls, recommendations will address areas where we believe controls could be improved.

We look forward to full cooperation from your staff during our assurance engagement.

[Other relevant information]

[Insert other information, such as fee arrangements, billings and other specific terms, as appropriate.]

Please sign and return the attached copy of this letter to indicate your acknowledgement of, and agreement with, the arrangements for our assurance engagement to report on the control procedures over your services to customers, including our respective responsibilities.

Yours faithfully,

(signed)

.....

Name and Title

Date

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Acknowledged on behalf of XYZ Service Organisation

(signed)

.....

Name and Title

Date

Draft

[Aus] Appendix 0B

(Ref: Para. 39)

Example Representation Letter

The following example of a representation letter is for guidance only and is not intended to be exhaustive or applicable to all situations.

Representation Letter for a Type 2 Engagement

[To auditor]

This representation letter is provided in connection with your assurance engagement to report on XYZ Service Organisation's [the type or name of] system (the system) for the period [date] to [date], set forth in XYZ Service Organisation's (XYZ) description of the system pages [bb-cc], for the purpose of expressing an opinion on the fair presentation of the description of the system, suitability of the design to achieve the control objectives and the operating effectiveness of controls throughout the period.

We confirm that, to the best of our knowledge and belief, having made such enquiries as we considered necessary for the purpose of appropriately informing ourselves:

Description of the System

1. We have fulfilled our responsibilities, as set out in the terms of the engagement dated [insert date], for the preparation of the description of the system pages [bb-cc] and the accompanying XYZ's assertion page [aa], including the completeness, accuracy and method of presentation of that description and assertion and we have a reasonable basis for making that assertion.
2. We have identified the risks that threaten achievement of the control objectives stated in the description of the system, and designed and implemented controls to provide reasonable assurance that those risks will not prevent achievement of the control objectives stated in the description of the system, and therefore the stated control objectives will be achieved.
3. The description of the system set out in our report fairly presents the system for processing customers' transactions throughout the period [date] to [date].

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

4. The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period [date] to [date].

Information Provided

5. We have provided you with:
- (a) access to all information of which we are aware that is relevant to the purposes of your engagement such as records, documentation and other matters;
 - (b) additional information that you have requested from us for the purpose of the assurance engagement; and
 - (c) unrestricted access to persons within XYZ from whom you determined it necessary to obtain evidence.
6. We have disclosed to you:
- (a) all known instances of non-compliance or suspected non-compliance with laws and regulations, fraud or suspected fraud and uncorrected deviations attributable to ABC that may effect one or more customers of [type of services];
 - (b) all design deficiencies in controls that we are aware of;
 - (c) all instances where controls have not operated as described that we are aware of; and
 - (d) any events subsequent to the period [date] to [date] up to [date of the assurance report] that could have a significant effect on your report.

Yours faithfully,

XYZ Service Organisation

.....
Management

.....
Management

Appendix 1

(Ref: Para. A47)

Example Service Organisation's Assertions

The following examples of service organisation's assertions are for guidance only and are not intended to be exhaustive or applicable to all situations.

Example 1: Type 2 Service Organisation's Assertion

Assertion by the Service Organisation

The accompanying description has been prepared for customers who have used [the type or name of] system and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial reports/statements. [Entity's name] confirms that:

- (a) The accompanying description at pages [bb-cc] fairly presents [the type or name of] system for processing customers' transactions throughout the period [date] to [date]. The criteria used in making this assertion were that the accompanying description:
 - (i) Presents how the system was designed and implemented, including:
 - The types of services provided, including, as appropriate, classes of transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
 - The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for customers.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- How the system dealt with significant events and conditions, other than transactions.
 - The process used to prepare reports for customers.
 - Relevant control objectives and controls designed to achieve those objectives.
 - Controls that we assumed, in the design of the system, would be implemented by customers, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
 - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions.
- (ii) Includes relevant details of changes to the service organisation's system during the period [date] to [date].
- (iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.
- (b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period [date] to [date]. The criteria used in making this assertion were that:
- (i) The risks that threatened achievement of the control objectives stated in the description were identified;
 - (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

prevent the stated control objectives from being achieved;
and

- (iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period [date] to [date].

Example 2: Type 1 Service Organisation's Assertion

The accompanying description has been prepared for customers who have used [the type or name of] system and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting. [Entity's name] confirms that:

- (a) The accompanying description at pages [bb-cc] fairly presents [the type or name of] system for processing customers' transactions as at [date]. The criteria used in making this assertion were that the accompanying description:
- (i) Presents how the system was designed and implemented, including:
- The types of services provided, including, as appropriate, classes of transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
 - The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports prepared for customers.
 - How the system dealt with significant events and conditions, other than transactions.
 - The process used to prepare reports for customers.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- Relevant control objectives and controls designed to achieve those objectives.
 - Controls that we assumed, in the design of the system, would be implemented by customers, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
 - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions.
- (ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.
- (b) The controls related to the control objectives stated in the accompanying description were suitably designed as at [date]. The criteria used in making this assertion were that:
- (i) The risks that threatened achievement of the control objectives stated in the description were identified; and
 - (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

[Aus] Appendix 1A

(Ref: Para. A47)

**Illustrative Example of a Service Organisation's Description
of the System Accompanying XYZ Service Organisation
Management's Assertion**

The following example of the service organisation's description of the system is illustrative only and is not intended to be exhaustive or applicable to all situations. The preparation and presentation of the description of the service organisation's system is the responsibility of management of the service organisation and the format is not prescribed by this standard, including this appendix. Management's description of the service organisation's system should be developed as appropriate to suit the individual circumstances of the assurance engagement.

**XYZ SERVICE ORGANISATION'S COMPUTER TIMESHARE
SYSTEM**

Services Provided

XYZ Service Organisation (XYZ) operates a data centre that provides its customers timeshare for on-line computer based systems. Batch generation of reports extracted from on-line data is also available upon request.

The data centre houses computer hardware and system software and accommodates operators responsible for day-to-day operations of the network, computer systems and production scheduling, the hardware, and an operations support function responsible for disk support, maintenance and back-up of data and software.

The System

The stated internal control objectives and related controls included in this report apply to XYZ operations as they relate only to computer timesharing services. Specifically excluded from this report are controls within individual systems, controls executed at customer premises and other services provided by XYZ, including data conversion services, custom application development and facilities management.

The effectiveness of controls performed by customers of XYZ should also be considered as part of the overall system of control relating to processing performed at the XYZ data centre.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

[Describe, as appropriate:¹⁹

- *The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.*
- *The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports prepared for customers.*
- *How the system dealt with significant events and conditions, other than transactions.*
- *The process used to prepare reports for customers.*

This may include a description of the flow of transactions or a flowchart],

[Controls at Subservice Organisations]²⁰

[XYZ Service Organisation uses [name of subservice organisation] to provide [type or name of] services, which form part of the [type or name of] system used by XYZ Service Organisation's customers. The [type or name of] services provided by [subservice organisation] are [describe the nature of the services provided]. XYZ Service Organisation's description of the system includes XYZ Service Organisation's monitoring controls over the operating effectiveness of the controls at [subservice organisation] and [includes/excludes]²¹ the relevant control objectives and related controls of [subservice organisation].]

We set out in this report the control objectives [specified by [identify law, regulation or another party]]²² and related controls implemented for the XYZ data centre of XYZ Service Organisation. The specific controls set out in the remainder of the report have been designed to achieve each of the control objectives. The controls have been in place throughout the period from [date] to [date] unless otherwise indicated.

¹⁹ Aspects of the system to be described here relate to the manner in which the system operates to provide services to customers but do not include specific controls which are designed to achieve the control objectives.

²⁰ Insert this section if XYZ Service Organisation uses a subservice organisation which performs some of the services provided to customers which use the system.

²¹ Use "includes" if the inclusive method is used and "excludes" if the carve-out method is used with respect to the subservice organisation's services.

²² Insert if control objectives are specified by law, regulation or another party.

Internal Control Objective

1. Effective segregation of duties exists at the XYZ data centre.

Related Controls²³

- 1.1 There is a formal organisation structure for all functions at the XYZ data centre. Each functional group reports to a separate manager, who in turn reports to the Senior Manager - Data Processing Services.

*[Period of operation: If the control has not been in operation the entire period or has changed, state the period during which the control was operating and the period during which the change was effective.]*²⁴

*[Complementary customer controls: Describe any complementary user entity controls contemplated in the design of the controls.]*²⁵

- 1.2 Segregation of functions exists for computer operations, systems support, hardware support, applications development and administrative functions.

Internal Control Objective

2. Physical security is restricted to prevent inadvertent or unauthorised access to computer facilities, software and documentation.

Related Controls

- 2.1 Security guards are in attendance 24 hours per day, 7 days per week. Entrances are either manned or locked and alarmed.
- 2.2 All exterior doors are locked, alarmed and subject to visual surveillance.
- 2.3 Access to and within the data centre is restricted by a cardkey security system that provides on-line monitoring of physical access

²³ Controls may include other aspects of the service organisation's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls which are designed to achieve the control objective and that are relevant to the services provided.

²⁴ This section should be inserted for each control which has not been in operation for the whole period or has changed during the period.

²⁵ This section should be inserted for each control for which there are complementary user entity controls contemplated in the design of the control.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

and intrusion. Procedures exist for security guards to monitor accesses and intrusions.

- 2.4 All authorised personnel are required to wear colour-coded badges that identify the individual and specify the areas to which access is allowed within the data centre.
- 2.5 Visitors must be signed in/out by an authorised individual and escorted whilst on the premises.

Internal Control Objective

- 3. Logical access is restricted to prevent inadvertent or unauthorised access to systems software, application programs and data.

Related Controls

- 3.1 Procedures exist to ensure all accesses are authorised.
- 3.2 All authorised personnel are issued unique user identification codes and are responsible for maintaining the corresponding passwords.
- 3.3 Access control software is implemented to restrict access and report violations of logical security.
- 3.4 Access violation reports are reviewed on a timely basis and followed-up.
- 3.5 Network transmissions originate from pre-determined terminal locations. Remote access is restricted.
- 3.6 Utilities identified as having special capabilities are restricted in their use and usage is monitored and justified.

Internal Control Objective

- 4. Systems software changes and enhancements are subject to authorisation and testing to maintain the integrity of the system software environment.

Related Controls

- 4.1 Responsibilities for the support and maintenance of system software are documented.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- 4.2 Changes and enhancements to system software components are scheduled.
- 4.3 All changes and enhancements to system software are authorised by the manager responsible for system software.
- 4.4 Testing of system software changes and enhancements are subject to pre-determined test criteria. Achievement of the criteria is required prior to implementation in the production environment.
- 4.5 Documentation for system software, including all changes and enhancements, exists in libraries organised by the software support function.

Internal Control Objective

- 5. An environmentally controlled facility exists to ensure continuity of data processing operations.

Related Controls

- 5.1 The data centre building is constructed on non-combustible materials.
- 5.2 The data centre is protected with fire, water and heat detection systems that are tested periodically. Fire suppression systems exist and are tested on a regular basis.
- 5.3 The data centre has an uninterruptible power supply (UPS) to prevent deviations in power supply to computer equipment and support facilities.
- 5.4 Preventive maintenance is carried out on a regular basis on the detection, air conditioning and fire suppression systems.

Internal Control Objective

- 6. Back-up procedures are adequate to ensure the continuity of processing in the event of a disaster.

Related Controls

- 6.1 A disaster recovery plan, designed to provide reasonable assurance that processing can be maintained, exists, is documented and maintained.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- 6.2 An off-site facility has been contracted for in order to execute the disaster recovery plan.
- 6.3 System software is backed up on a weekly basis and stored off-site. Application programs and data are backed up daily and stored off-site. Documentation is backed up monthly and stored off-site.
- 6.4 On-site back-ups exist to facilitate the resumption of processing operations in the event of minor interruptions in processing.
- 6.5 The disaster recovery plan is tested at least once on an annual basis.

Internal Control Objective

- 7. Problems relating to data centre operations, including the communications network, are identified and resolved on a timely basis.

Related Controls

- 7.1 Schedules establishing the operations of the data centre are pre-determined and authorised.
- 7.2 All special requests of the operations support function must be documented and authorised.
- 7.3 Performance of the data centre operations, including the communications network, is monitored on a regular basis.
- 7.4 Problems identified with computer operations are logged and the status is monitored to resolution.
- 7.5 Operations support prepares a weekly report describing major incidents and summarising system performance as compared to established performance criteria. The report is reviewed by data centre management.

Appendix 2

(Ref: Para. A47)

Example Service Auditor's Assurance Reports

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

Example 1: Type 2 Service Auditor's Assurance Report

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

To: XYZ Service Organisation

Scope

We have been engaged to report on XYZ Service Organisation's description at pages [bb-cc] of its [type or name of] system for processing customers' transactions throughout the period [date] to [date] (the description), and on the design and operation of controls related to the control objectives stated in the description.²⁶

XYZ Service Organisation's Responsibilities

XYZ Service Organisation is responsible for: preparing the description and accompanying assertion at page [aa], including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on XYZ Service Organisation's description and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation*, issued by the Auditing and Assurance Standards Board. That standard requires that we comply with relevant ethical requirements and plan and

²⁶ If some elements of the description are not included in the scope of the engagement, this is made clear in the assurance report.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on our judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation and described at page [aa].

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

Limitations of Controls at a Service Organisation

XYZ Service Organisation's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation 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 organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described at page [aa]. In our opinion, in all material respects:

- (a) The description fairly presents the [the type or name of] system as designed and implemented throughout the period from [date] to [date];
- (b) The controls related to the control objectives stated in the description were suitably designed throughout the period from [date] to [date];
and

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

- (c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from [date] to [date].

Description of Tests of Controls

The specific controls 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 customers who have used XYZ Service Organisation's [type or name of] system, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial reports/statements.

[Service auditor's signature]

[Date of the service auditor's assurance report]

[Service auditor's address]

Example 2: Type 1 Service Auditor's Assurance Report

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

To: XYZ Service Organisation

Scope

We have been engaged to report on XYZ Service Organisation's description at pages [bb-cc] of its [type or name of] system for processing customers' transactions as at [date] (the description), and on the design of controls related to the control objectives stated in the description.²⁷

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

XYZ Service Organisation's Responsibilities

XYZ Service Organisation is responsible for: preparing the description and accompanying assertion at page [aa], including the completeness, accuracy and method of presentation of the description and the assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on XYZ Service Organisation's description and on the design of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3402 *Assurance Reports on Controls at a Service Organisation*, issued by the Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed in all material respects.

An assurance engagement to report on the description and design of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system,

²⁷ If some elements of the description are not included in the scope of the engagement, this is made clear in the assurance report.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

and the design of controls. The procedures selected depend on our judgement, including the assessment that the description is not fairly presented, and that controls are not suitably designed. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organisation and described at page [aa].

As noted above, 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 Controls at a Service Organisation

XYZ Service Organisation's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation 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 outlined in this report. The criteria we used in forming our opinion are those described at page [aa]. In our opinion, in all material respects:

- (a) The description fairly presents the [the type or name of] system as designed and implemented as at [date]; and
- (b) The controls related to the control objectives stated in the description were suitably designed as at [date].

Intended Users and Purpose

This report is intended only for customers who have used XYZ Service Organisation's [type or name of] system, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

[Service auditor's signature]

[Date of the service auditor's assurance report]

[Service auditor's address]

Draft

Appendix 3

(Ref: Para. A47)

Example Modified Service Auditor's Assurance Reports

The following examples of modified reports are for guidance only and are not intended to be exhaustive or applicable to all situations. They are based on the examples of reports in Appendix 2.

Example 1: Qualified opinion – the service organisation's description of the system is not fairly presented 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 description states at page [mn] that XYZ Service Organisation uses operator identification numbers and passwords to prevent unauthorised access to the system. Based on our procedures, which included enquiries of staff personnel and observation of activities, we have determined that operator identification numbers and passwords are employed in Applications A and B but not in Applications C and D.

Qualified Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion were those described in XYZ Service Organisation'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 control objectives stated in the service organisation’s description of its system will be achieved if the controls operate effectively

...

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

As discussed at page [mn] of the accompanying description, from time to time XYZ Service Organisation 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 authorised 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 authorised reviewer prior to implementing the changes.

Qualified Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion were those described in XYZ Service Organisation’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 2 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.

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Basis for Qualified Opinion

XYZ Service Organisation 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 [date] to [date] 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 [date] to [date]. XYZ 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 [date] to [date].

Qualified Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion were those described in XYZ Service Organisation’s assertion at page [aa]. In our opinion, except for the matter described in the Basis for Qualified Opinion paragraph:

...

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 Organisation states in its description that it has automated controls in place to reconcile loan payments received with the output generated. However, electronic records of the performance of this reconciliation for the period from [date] to [date] 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 [date] to [date].

Standard on Assurance Engagements ASAE 3402
Assurance Reports on Controls at a Service Organisation

Qualified Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion were those described in XYZ Service Organisation's assertion at page [aa]. In our opinion, except for the matter described in the Basis for Qualified Opinion paragraph:

- (a) ...