ASAE 3150
(December 2022)

Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls*

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 Auditing and Assurance Standards Board (AUASB) website: www.auasb.gov.au

Contact Details

Auditing and Assurance Standards Board
Level 20, 500 Collins Street
Melbourne Victoria AUSTRALIA 3000

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

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

COPYRIGHT

© 2022 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 as being the AUASB.

Requests and enquiries concerning reproduction and rights for commercial purposes should be addressed to the Technical Director, Auditing and Assurance Standards Board, PO Box 204, Collins Street West, Melbourne, Victoria 8007 or sent to enquiries@auasb.gov.au. Otherwise, no part of this 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.

This ASAE reflects certain aspects of other Australian ASAEs, which reproduce substantial parts of the corresponding International Standards on Assurance Engagements (ISAEs) issued by the International Auditing and Assurance Standards Board (IAASB) and published by the International Federation of Accountants (IFAC), in the manner described in the statement of Conformity with International Standards on Assurance Engagements. The AUASB acknowledges that IFAC is the owner of copyright of material in the ISAEs that is incorporated in this ASAE throughout the world.

All existing rights in this material are reserved outside Australia. Reproduction outside Australia in unaltered form (retaining this notice) is permitted for personal and non-commercial use only.

ISSN 1834-4860

CONTENTS

PREFACE

Reasons for Issuing ASAE 3150

The AUASB issues Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls*, pursuant to the requirements of the legislative provisions explained below.

The AUASB is an independent, non-corporate Commonwealth entity 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, the AUASB is required to have regard to any programme initiated by the International Auditing and Assurance Standards Board (IAASB) for the revision and enhancement of International Standards on Auditing and to make appropriate consequential amendments to the Australian Auditing Standards.

The amendments arise from changes made by the IAASB to ISQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, ISQM 2 *Engagement Quality Reviews* and ISA 220 (Revised) *Quality Management for an Audit of Financial Statements*.

Main Features

This Standard on Assurance Engagements establishes requirements and provides application and other explanatory material regarding the conduct of and reporting on engagements to provide assurance on controls. The standard replaces Auditing Standard AUS 810 *Special Purpose Reports on the Effectiveness of Control Procedures*, issued by the former AuASB and last revised in July 2002. This Standard on Assurance Engagements facilitates conformity with current AUASB Standards and revised ASAE 3000 *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*. The standard reflects best practice and clarifies how to scope, conduct and report on an assurance engagement on controls, to ensure that assurance engagement quality is maintained and where necessary improved.

This Standard on Assurance Engagements will replace the current ASAE 3150 issued by the AUASB in January 2015.

AUTHORITY STATEMENT

The Auditing and Assurance Standards Board (AUASB) formulates this Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls*, 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 101 *Preamble to AUASB Standards*, which sets out how AUASB Standards are to be understood, interpreted and applied.

Dated: 6 September 2022

W R Edge
Chair - AUASB

Conformity with International Standards on Assurance Engagements

This Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls* has been formulated for Australian public interest purposes and there is no equivalent International Standard on Assurance Engagements (ISAE), issued by the International Auditing and Assurance Standards Board (IAASB), an independent standard-setting board of the International Federation of Accountants (IFAC).

This Standard does, however, reflect certain aspects of other Australian ASAEs, which reproduce substantial parts of the equivalent ISAEs issued by the IAASB and published by IFAC, including ISAE 3000 *Assurance Engagements Other than Audits or Reviews of Historical Financial Information* and ISAE 3402 *Assurance Reports on Controls at a Service Organization*.

This Standard incorporates terminology and definitions used in Australia.

STANDARD ON ASSURANCE ENGAGEMENTS ASAE 3150

Assurance Engagements on Controls

Application

1. This Standard on Assurance Engagements applies to assurance engagements to provide an assurance report on controls at an entity, except for engagements to which ASAE 3402[1] is applicable.[2] (Ref: Para. A1)

Operative Date

2. This Standard on Assurance Engagements is operative for assurance engagements commencing on or after 15 December 2022.

Introduction

Scope of this Standard on Assurance Engagements

3. This Standard on Assurance Engagements (ASAE) deals with assurance engagements undertaken by an assurance practitioner to provide an assurance report on the suitability of the design of controls to achieve identified control objectives, and, if applicable, fair presentation of the description of the system, implementation of the controls as designed and/or operating effectiveness of controls as designed.

4. This ASAE addresses engagements on controls, except those engagements to which ASAE 3402 applies: (Ref: Para. A2-A7)

   (a) over any subject matter, whether directed at operations, external reporting, contractual compliance or regulatory compliance; (Ref: Para. A3)

   (b) evaluated against the achievement of either overall or specific control objectives;

   (c) covering one or more component/s of control;[3]

   (d) providing a limited or reasonable assurance conclusion;

   (e) for either restricted use, by those charged with governance of the entity or specified third parties, or to be publicly available; (Ref: Para. A5)

   (f) either based on an attestation engagement or a direct engagement; (Ref: Para. 17(a), 17(o), A6)

---

1 See ASAE 3402 *Assurance Reports on Controls at a Service Organisation*, which 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 that provides a service to user entities that is likely to be relevant to user entities' internal control as it relates to financial reporting.

2 The assurance practitioner applies ASA 315 *Identifying and Assessing the Risks of Material Misstatement* when obtaining an understanding of controls for the purposes of the audit of a financial report, standards on review engagements when obtaining an understanding of controls for the purposes of the review of a financial report or ASAE 3000 *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, and any subject matter specific standard when understanding controls for the purposes of an assurance engagement on subject matters other than historical financial information.

3 Control components will depend on the controls framework applied. For example the control components in the Treadway Commission's *Internal Control Integrated Framework 2013* (COSO Framework) are: the control environment, risk assessment, control activities, information and communication or monitoring activities and in the COBIT 5 Framework the equivalent are the following enablers: principles, policies and frameworks; processes; organisational structures; culture, ethics and behaviour; information; services, infrastructure and applications; and people, skills and competencies.

(g) to conclude either:

(i) as at a specified date, on the suitability of the design of controls to achieve the identified control objectives, and, if included in the scope of the engagement:

a. fair presentation of the description of the system; and/or

b. implementation of the controls as designed; or

(ii) throughout the period, on the suitability of the design of controls to achieve identified control objectives and operating effectiveness of controls as designed, and, if included in the scope of the engagement, fair presentation of the description of the system.

5. The scope of an engagement on controls includes either implementation at a specified date or operating effectiveness over the period but not usually both, because implementation is inherent in testing operating effectiveness.

6. Agreed-upon procedures engagements, where procedures are conducted and factual findings are reported but no conclusion is provided, and consulting engagements, for the purpose of providing advice, on controls are not assurance engagements and are not dealt with in this ASAE. Agreed-upon procedures engagements are addressed under Standard on Related Services, ASRS 4400.[4]

Nature of Engagements

7. Assurance engagements on controls may include, but are not limited to:

(a) compliance with contractual requirements agreed with customers, investors, financiers, purchasers or government for controls to achieve identified control objectives at an entity, such as controls over health and safety, ethics, privacy and security of data and information technology (IT) accessibility;

(b) compliance with regulatory requirements, such as:

(i) Australian Prudential Regulation Authority (APRA) reporting requirements for limited assurance on controls over compliance, data reliability and other specified matters for general insurers,[5] authorised deposit-taking institutions,[6] life companies,[7] superannuation entities[8] and APRA–regulated group level 3 heads;[9] or

(ii) legislative requirements for assurance reports on controls at certain government entities;

(c) concluding on operational or compliance controls at a service organisation to meet the needs of user auditors, except for financial reporting controls (Ref: Para. 1, A1);[10] or

[4] See ASRS 4400 *Agreed-upon Procedures Engagements.*
[5] See Guidance Statement GS 004 *Audit Implications of Prudential Reporting Requirements for General Insurers and Insurance Groups* and Prudential Standard GPS 310 *Audit and Related Matters.*
[6] See Guidance Statement GS 012 *Prudential Reporting Requirements for Auditors of Authorised Deposit-taking Institutions* and Prudential Standard APS 310 *Audit and Related Matters.*
[7] See Guidance Statement GS 017 *Prudential Reporting Requirements for Auditors of a Life Company* and Prudential Standard LPS 310 *Audit and Related Matters.*
[8] See Guidance Statement GS 002 *Audit Implications of Prudential Reporting Requirements for Registrable Superannuation Entities* and Prudential Standard SPS 310 *Audit and Related Matters.*
[9] See Prudential Standard 3PS 310 *Audit and Related Matters.*
[10] Financial reporting controls at a service organisation are addressed in ASAE 3402 and so are excluded from this ASAE.

(d) voluntary engagements initiated by the entity on its own controls over services, activities undertaken or functions which it provides.

8. The control framework applied in designing the controls is relevant when identifying the components of control and overall control objectives to be addressed in the scope of the engagement and as a basis for the development of specific control objectives. The control framework may be derived from:

(a) legislation or regulation;

(b) a publicly available framework, such as the Committee of Sponsoring Organizations of the Treadway Commission's *Internal Control Integrated Framework 2013* (COSO Framework) or COBIT 5;

(c) industry standard, developed specifically to meet the relevant industry; or

(d) in-house development to meet the entity's needs.

Relationship with ASAE 3000, Other Pronouncements and Other Requirements

9. The assurance practitioner is required to comply with ASAE 3000 and this ASAE when performing assurance engagements on controls, other than engagements required to be conducted under ASAE 3402. This ASAE supplements, but does not replace, ASAE 3000, and expands on how ASAE 3000 is to be applied to limited and reasonable assurance engagements on controls. This ASAE applies the requirements in ASAE 3000 to attestation engagements and adapts those requirements, as necessary, to direct engagements on controls. ASAE 3000 includes requirements in relation to such topics as engagement acceptance, planning, obtaining evidence and documentation that apply to all assurance engagements, including engagements conducted in accordance with this ASAE. The *Assurance Framework*, which defines and describes the elements and objectives of an assurance engagement, provides the context for understanding this ASAE and ASAE 3000.

10. Compliance with ASAE 3000 requires, among other things, that the assurance practitioner complies with relevant ethical requirements related to assurance engagements, or other professional requirements, or requirements in law or regulation, that are at least as demanding.[11] (Ref: Para. 19) It also requires the lead assurance practitioner[12] to be a member of a firm that applies ASQM 1 or other professional requirements, or requirements in law or regulation, that are at least as demanding as ASQM 1.[13]

11. An assurance engagement performed under this ASAE may be part of a larger engagement. In such circumstances, this ASAE is relevant only to the portion of the engagement relating to assurance on controls.

12. If multiple standards are applicable to an assurance engagement on controls, the assurance practitioner applies, in addition to ASAE 3000, either:

(a) if the engagement can be separated into parts, the standard relevant to each part of the engagement; or

(b) if the engagement cannot be separated into parts, the standard which is most directly relevant to the subject matter.

---

[11] See ASAE 3000, paragraphs 3(a), Aus 20.1 and 34 and ASA 102 *Compliance with Ethical Requirements when Performing Audits, Reviews and Other Assurance Engagements*.

[12] The term "lead assurance practitioner" is referred to in ASQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements* as the "engagement partner".

[13] See ASAE 3000, paragraphs 3(b) and 31(a).

13. Assurance conclusions on controls are often required by regulators or users in conjunction with assurance conclusions on financial reports, other historical financial information, compliance and/or other subject matters. In addition, service auditors may be engaged to report under ASAE 3402, on controls at a service organisation that are likely to be relevant to user entities' internal control as it relates to financial reporting, as well as to report under this ASAE, on controls over operational or compliance requirements, as agreed in a service level agreement. In these engagements the subject matter, criteria against which that subject matter is evaluated and the level of assurance sought may vary, in which case different standards will apply. Assurance reports can include separate sections for each subject matter, criteria or level of assurance in order that the different matters concluded upon are clearly differentiated. (Ref: Para. A8)

14. A table showing the AUASB Standards to apply to assurance engagements on controls depending on the subject matter and engagement circumstances is contained in Appendix 3.

Objectives

15. The objectives of the assurance practitioner for an assurance engagement on controls are:

    (a) to obtain limited or reasonable assurance about whether, in all material respects, based on suitable criteria, either:

        (i) as at a specified date, the controls were suitably designed, to achieve the identified control objectives and, if included in the scope of the engagement:

            a. the entity's description of the system of controls fairly presents the system;[14] and/or

            b. the controls were implemented as designed; or

        (ii) throughout the period, the controls were suitably designed to achieve the identified control objectives, the controls operated effectively as designed and, if included in the scope of the engagement, the entity's description of its system fairly presents the system;[14] and

    (b) to express a conclusion through a written report on the matters in (a) above which expresses either a reasonable or limited assurance conclusion and describes the basis for the conclusion.

16. In conducting the assurance engagement, the objectives of the assurance practitioner under ASAE 3000[15] include: "to obtain either reasonable or limited assurance, as appropriate, about whether the subject matter information is free from material misstatement". The subject matter information in a controls engagement is the outcome of the evaluation of the design, and/or the description, implementation or operating effectiveness of controls against the criteria. The evaluation is conducted:

    (a) in an attestation engagement, by the responsible party or evaluator, and presented in a Statement, which addresses whether the controls are suitably designed to achieve identified control objectives, and if applicable, the description is fairly presented, the controls are implemented as designed and/or operated effectively. The objective of the assurance practitioner is to obtain reasonable or limited assurance about whether the Statement is free from material misstatement, although the assurance practitioner's conclusion may be expressed in terms of the subject matter; or

[14] Assurance over the description of the system is optional and is included if that description will be available to users.
[15] See ASAE 3000, paragraph 10.

(b) in a direct engagement, by the assurance practitioner and presented in the assurance report, therefore, no Statement is prepared by the responsible party or evaluator. The objectives of the assurance practitioner are to obtain reasonable or limited assurance about whether the controls are suitably designed to achieve identified control objectives, and, if included in the scope of the engagement, the description is fairly presented, the controls were implemented as designed and/or operated effectively.

Definitions

17. For the purposes of this ASAE, terms have the same meaning as in ASAE 3000 and in addition, the following terms have the meanings attributed below:

(a) Attestation engagement on controls—A reasonable or limited assurance engagement in which a party other than the assurance practitioner, being the responsible party or evaluator, evaluates the design against the control objectives, and, if included in the scope of the engagement, the description, implementation or operating effectiveness of controls, against the design. The outcome of that evaluation is provided in a Statement, which may either be available to the intended users or may be presented by the assurance practitioner in the assurance report. The assurance practitioner's conclusion may be phrased in terms of: (Ref: Para. A6)

(i) the design, and/or description, implementation or operating effectiveness of controls and the control objectives; or

(ii) the Statement of the responsible party or evaluator.

(b) Anomaly—A deviation in a sample that is demonstrably not representative of deviations in a population.

(c) Carve-out method—A method of dealing with controls operating at a third party, which are integral to the system or control component which is subject to the engagement, whereby that third party's relevant control objectives and related controls are excluded from the scope of the assurance practitioner's engagement. The scope of the assurance practitioner's engagement includes controls at the entity to monitor the effectiveness of controls which form part of the entity's system, operating at the third party.

(d) Compensating control—A control which makes up for a deficiency in another control in mitigating the risks that threaten achievement of a control objective.

(e) Complementary user entity controls—Controls that an entity, which is a service organisation, assumes, in the design of its service, will be implemented by user entities or clients, and which, if necessary to achieve control objectives stated in the entity's description of its system, are identified in that description.

(f) Components of control—The integrated components which comprise the system of control, as defined by the control framework applied. (Ref: Para. A9)

(g) Control objective—The aim or purpose of a particular aspect of controls. Control objectives relate to risks that controls seek to mitigate and may be categorised by the framework applied, such as operational (economy, effectiveness and efficiency), reporting (statutory or management, financial or non-financial) or compliance (adherence to laws and regulations or contractual obligations).

(h) Control or internal control—The process designed, implemented and maintained by those charged with governance, management and other personnel to mitigate the risks which may prevent achievement of control objectives relating to the entity's system. Controls included in the scope of the assurance engagement may comprise any aspects

of one or more components of control over an area(s) of activity within a defined boundary, such as the group, entity, facility or location.

(i) Criteria—The benchmarks used to measure or evaluate the underlying subject matter. The "applicable criteria" are the criteria used for the particular engagement.

(j) Description of the system—A document prepared by the responsible party and provided to users, if included in the scope of the engagement, describing the entity's system, within which the controls to be concluded upon operate, including identification of: the functions or services covered; the period or date to which the description relates; control objectives and details of, or reference to documentation detailing, the controls designed to achieve those objectives. The entity's functions or services may be identified by geographic, operational or functional boundaries. A description of the system is distinct from documentation prepared by the responsible party or assurance practitioner, as the description is part of the subject matter of the engagement, which, if included in the scope of the engagement, is made available to users and concluded upon by the assurance practitioner. A description may be included in the scope of an attestation or direct engagement, however in a direct engagement no attestation is provided by the responsible party or evaluator with respect to whether the description is fairly presented.

(k) Deficiency in design of controls—An inadequacy or omission in the design of a control/s that, in the assurance practitioner's professional judgement, means the control/s is not designed suitably to mitigate the risks that threaten achievement of the identified control objective/s.

(l) Deficiency in implementation of controls—Instances where a control was not implemented as designed that, in the assurance practitioner's professional judgement, mean the control/s, once in operation, may not operate effectively as designed to achieve the identified control objective/s.

(m) Deviation in operating effectiveness of controls—Instances where a control was not operating as designed.

(n) Direct controls—Controls which directly address the risks of a control objective not being achieved, by detecting, preventing or correcting a failure to achieve a control objective on a timely basis.

(o) Direct engagement on controls—A reasonable or limited assurance engagement in which the assurance practitioner evaluates the design of the controls against the control objectives, and, if included in the scope of the engagement, the description, implementation and/or operating effectiveness of controls against the design. The outcome of the assurance practitioner's evaluation (the subject matter information) is expressed in the assurance practitioner's conclusion. (Ref: Para. A6)

(p) Engaging party—The party(ies) that engages the assurance practitioner to perform the assurance engagement.

(q) Entity's system (or the system)—The policies and procedures designed and implemented by the entity to provide the functions or services covered by the assurance practitioner's report, including the control objectives which address the overall objectives relevant to those functions or services and the controls designed to mitigate the risks that threaten achievement of those objectives.

(r) Evaluator—The party(ies) who evaluates the underlying subject matter against the criteria. The evaluator possesses expertise in the underlying subject matter.

(s) Firm—A sole assurance practitioner, partnership or corporation or other entity of individual assurance practitioners. "Firm" should be read as referring to its public sector equivalents where relevant.

(t) Fraud—An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.

(u) Fraud risk factors—Events or conditions that indicate an incentive or pressure to commit fraud or provide an opportunity to commit fraud.

(v) Implementation—The process of putting controls into effect by deployment or roll-out of controls to enable their operation as designed.

(w) Inclusive method—A method of dealing with the controls operating at a third party, which are integral to the system or control component which is subject to the assurance engagement, whereby the third party's relevant control objectives and related controls are included in the scope of the assurance practitioner's engagement.

(x) Indirect controls—Controls which do not directly address the risks of a control objective not being achieved, but have an impact on the effectiveness of direct controls in detecting, preventing or correcting a failure to achieve a control objective on a timely basis.

(y) Intended users—The individual(s) or organisation(s), or group(s) thereof that the assurance practitioner expects will use the assurance report. In some cases, there may be intended users other than those to whom the assurance report is addressed.

(z) Internal audit function—A function of an entity that performs assurance and consulting activities designed to evaluate and improve the effectiveness of the entity's governance, risk management and internal control processes.

(aa) Internal auditors—Those individuals who perform the activities of the internal audit function. Internal auditors may belong to an internal audit department or equivalent function, out-sourcing entity or co-sourced from both internal and out-sourced resources.

(bb) Limited assurance engagement—An assurance engagement in which the assurance practitioner reduces engagement risk to a level that is acceptable in the circumstances of the engagement, but where that risk is greater than for a reasonable assurance engagement, as the basis for expressing a conclusion in a form that conveys whether, based on the procedures performed and evidence obtained, a matter(s) has come to the assurance practitioner's attention to cause the assurance practitioner to believe the subject matter information or subject matter is materially misstated. The nature, timing and extent of procedures performed in a limited assurance engagement is limited compared with that necessary in a reasonable assurance engagement but is planned to obtain a level of assurance that is, in the assurance practitioner's professional judgement, meaningful. To be meaningful, the level of assurance obtained by the assurance practitioner is likely to enhance the intended users' confidence about the subject matter information or subject matter to a degree that is clearly more than inconsequential.

(cc) Long-form report—Assurance report including other information and explanations that are intended to meet the information needs of users but not to affect the assurance practitioner's conclusion. In addition to the matters required to be contained in the assurance practitioner's report, as set out in paragraph 89, long-form reports may describe in detail matters such as:

(i) the terms of the engagement;

(ii) the criteria being used, such as the specific control objectives and controls as designed to achieve each objective;

(iii) descriptions of the tests of controls that were performed;

(iv) findings relating to the the tests of controls that were performed or particular aspects of the engagement;

(v) details of the qualifications and experience of the assurance practitioner and others involved with the engagement;

(vi) disclosure of materiality levels; or

(vii) recommendations.

The assurance practitioner may find it helpful to consider the significance of providing such information to meet the needs of the intended users. As required by paragraph 90, additional information is clearly separated from the assurance practitioner's conclusion and worded in such a manner as make it clear that it is not intended to alter or detract from that conclusion.

(dd) Material control—A control which is necessary to mitigate the risk of a control objective not being achieved and for which there are no or insufficient compensating controls. The relevant control objectives are those at the level to be concluded on in the assurance report, whether overall or specific control objectives.

(ee) Misstatement—

(i) In an attestation engagement, a difference between the responsible party or evaluator's Statement[16] and the appropriate evaluation of the design of controls against the control objectives[17], and/or the description, implementation or operating effectiveness of controls against the design[17], which is expressed either as a misstatement in the responsible party or evaluator's Statement, or as a deficiency in the suitability of the design, misstatement in the description, deficiency in implementation or deviation in operating effectiveness of controls.

(ii) In a direct engagement, a difference between the design and a design suitable to achieve the control objectives[17] and/or a difference between the description, implementation or operating effectiveness of controls and the design,[17] in so far as it is suitable, which is expressed as a deficiency in the suitability of the design of controls to achieve the control objectives, misstatement in the description, deficiency in the implementation or deviation in the operating effectiveness of controls as designed.

Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions.

(ff) Misstatement in the description of the system—An inaccuracy, inadequacy or omission in the description, including in the identification of the boundaries and other identifying characteristics of the system, the control components described, the areas of activity encompassed and the controls as designed and/or implemented.

---

[16] The "subject matter information", as referred to in ASAE 3000 paragraph 12(x), is the responsible party or evaluator's Statement in an attestation engagement on controls.

[17] The "criteria", as referred to in ASAE 3000 paragraph 12(c), are the control objectives for the evaluation of the design of controls and the design of controls for evaluating the description, implementation or operating effectiveness of controls, in an attestation or direct engagement on controls.

(gg) Overall control objectives—Explicit or implicit assertions by the responsible party with respect to the subject matter, that in an assurance engagement on controls, represent the broad objectives or purpose of the controls, in the context of the control component and system included in the scope of the engagement.

(hh) Population—The entire set of instances of a particular control from which a sample is selected and about which the assurance practitioner wishes to draw conclusions.

(ii) Pervasive—The effect or possible effect on the system of controls of, identified or undetected, deficiencies in the design of controls, misstatements in the description, deficiencies in implementation as designed or deviations in operating effectiveness as designed. Pervasive effects on the controls system are those that, in the assurance practitioner's judgement:

(i) Are not confined to certain overall or specific control objectives, areas of activity, components of controls or controls; or

(ii) If so confined, represent or could represent a substantial proportion of the system of controls included in the scope of the engagement.

(jj) Reasonable assurance engagement—An assurance engagement in which the assurance practitioner reduces engagement risk to an acceptably low level in the circumstances of the engagement as the basis for the assurance practitioner's conclusion. The assurance practitioner's conclusion is expressed in a form that conveys the assurance practitioner's opinion on the outcome of the measurement or evaluation of the underlying subject matter against criteria.

(kk) Representation—Statement by the responsible party, either oral or written, provided to the assurance practitioner to confirm certain matters or to support other evidence. A representation is additional to but may be provided in combination with the responsible party's or evaluator's Statement provided in an attestation engagement, as set out in paragraph 17(rr).

(ll) Responsible party—The party responsible for the underlying subject matter, being the design, description, implementation or operating effectiveness of controls in an assurance engagement on controls.

(mm) Sampling—The application of assurance procedures to less than 100% of items within a population of relevance to the engagement such that all sampling units have a chance of selection in order to provide the assurance practitioner with a reasonable basis on which to draw conclusions about the entire population.

(nn) Sampling risk—The risk that the assurance practitioner's conclusion based on a sample may be different from the conclusion if the entire population were subjected to the same assurance procedure. Sampling risk can lead to two types of erroneous conclusions:

(i) That the controls are designed more suitably, the description is presented more fairly or the controls are operating more effectively than they actually are. The assurance practitioner is primarily concerned with this type of erroneous conclusion because it affects the engagement's effectiveness and is more likely to lead to an inappropriate assurance conclusion.

(ii) That controls are less effective than they actually are. This type of erroneous conclusion affects the engagement's efficiency as it would usually lead to additional work to draw a conclusion.

(oo) Service organisation—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 relevant external reporting, whether financial, emissions and energy, carbon offsets, compliance or other reporting.

(pp) Short-form report—Assurance report including only the matters required under paragraph 89 of this ASAE.

(qq) Specific control objective—Control objective expressed in sufficient detail such that controls can be designed to achieve that objective directly without further breakdown.

(rr) Statement—The outcome in writing of the responsible party or evaluator's evaluation of the suitability of the design of controls to achieve the control objectives, and, if included in the scope of the engagement, the fair presentation of the description of the system, implementation of controls as designed or operating effectiveness of controls as designed, provided to the assurance practitioner in an attestation engagement. A Statement is the subject matter information in an attestation engagement on controls.

(ss) Subject matter information—The outcome of the measurement or evaluation of the underlying subject matter against the criteria. In an assurance engagement on controls the subject matter information is the Statement of the responsible party or evaluator in an attestation engagement or the assurance practitioner's conclusion in a direct engagement, providing the outcome of their evaluation.

(tt) Subject matter or underlying subject matter—The controls within the system designed to achieve the control objectives, and, if included in the scope of the engagement, the description of the system, the controls implemented or the controls in operation.

(uu) System—The function or service at the entity, location or operational facility for which the controls are being reported upon by the assurance practitioner.

(vv) Test of controls—A procedure designed to evaluate the design, description, implementation or operating effectiveness of controls in achieving the identified control objectives.

(ww) Tolerable rate of deviation—A rate of deviation in the operation of control procedures as designed in respect of which the assurance practitioner seeks to obtain an appropriate level of assurance that the rate of deviation set by the assurance practitioner is not exceeded by the actual rate of deviation in the population.

(xx) User entity—An entity that uses a service organisation.

Requirements

Applicability of ASAE 3000

18. The assurance practitioner shall not represent compliance with this ASAE unless the assurance practitioner has complied with the requirements of this ASAE and ASAE 3000, adapted as necessary in the case of direct engagements. ASAE 3000 contains requirements and application and other explanatory material specific to attestation assurance engagements but it also applies to direct assurance engagements, adapted as necessary in the engagement circumstances.[18] If this ASAE makes reference to a requirement in ASAE 3000, that requirement shall be applied to both attestation and direct engagements, unless specified otherwise. (Ref: Para. A6)

[18] See ASAE 3000, paragraph 2.

Ethical Requirements

19. As required by ASAE 3000, the assurance practitioner shall comply with relevant ethical requirements related to assurance engagements, or other professional requirements, or requirements imposed by law or regulation, that are at least as demanding.[19] (Ref: Para. A10)

Acceptance and Continuance

Preconditions for the Assurance Engagement

20. The assurance practitioner shall accept or continue an assurance engagement on controls only in the circumstances required by ASAE 3000,[20] including that the preconditions for an assurance engagement are present, unless required to accept the engagement by law or regulation. (Ref: Para. A11-A14)

Assessing the Appropriateness of the Subject Matter

21. When establishing whether the preconditions for an assurance engagement as required by ASAE 3000 are present, the assurance practitioner is required to assess the appropriateness of the subject matter.[21] In doing so, the assurance practitioner shall determine whether the control components and specific controls are identifiable, the controls are capable of consistent evaluation against the control objectives and the scope of the controls within the assurance engagement provide an appropriate basis for that engagement. If the subject matter is not appropriate, the assurance practitioner shall not accept the engagement or, if this is determined after accepting the engagement, either withdraw from the engagement or issue a modified conclusion. (Ref: Para. A15)

Assessing the Suitability of the Criteria

22. When establishing whether the preconditions for an assurance engagement as required by ASAE 3000 are present, the assurance practitioner shall determine the suitability of the criteria expected to be applied, whether the criteria are provided by the engaging party, as in an attestation engagement, or are to be identified, selected or developed by the assurance practitioner, as in a direct engagement, including that they exhibit the characteristics set out in ASAE 3000.[22] The main criteria are: (Ref: Para. A16-A26)

    (a) control objectives, for evaluating the design of the controls; and

    (b) controls, necessary to achieve the control objectives, as designed, for evaluating the description of the system, implementation of controls or operating effectiveness.

23. If the assurance practitioner considers that the identified criteria are unsuitable, the assurance practitioner shall either:

    (a) agree on suitable criteria with the engaging party prior to accepting or continuing with the engagement. If unable to agree on suitable criteria, the assurance practitioner shall withdraw from the engagement; or

    (b) issue a modified conclusion, either qualified or a disclaimer depending on the extent of the unsuitable criteria, if the assurance practitioner is required to perform the engagement using the unsuitable criteria, such as under a legislative mandate.

[19] See ASAE 3000, paragraphs Aus 20.1 and ASA 102.
[20] See ASAE 3000, paragraphs 21-30.
[21] See ASAE 3000, paragraph 24(b)(i).
[22] See ASAE 3000, paragraph 24(b).

Agreeing on the Terms of the Engagement

24. The parties to the engagement shall agree on the terms of the assurance engagement in writing, as required by ASAE 3000,[23] and the assurance practitioner shall obtain the agreement of the responsible party, if they are a party to the engagement, that it acknowledges and understands its responsibility: (Ref: Para. A27)

    (a) in an attestation engagement,

        (i) for evaluating the suitability of the design of controls to achieve the identified control objectives, and if applicable, the presentation of the description, implementation and/or operating effectiveness of controls, as designed, which are the subject matter of the assurance engagement, and providing a written Statement regarding the outcome of that evaluation;

        (ii) for having a reasonable basis for the written Statement; (Ref: Para. A37-A39)

    (b) in both an attestation and a direct engagement:

        (i) for identifying suitable control objectives and whether they were specified by law, regulation, contract, another party (for example, a user group or a professional body) or developed by the responsible party or assurance practitioner;

        (ii) for identifying the risks that threaten achievement of those control objectives;

        (iii) for designing controls to mitigate those risks so they will not prevent achievement of the identified control objectives, and therefore the control objectives will be achieved;

        (iv) if included in the scope of the engagement:

            a. for preparing a description of the system, including identification of any controls operated by a third party, service or sub-service organisation, which may be material to the engagement, and whether the inclusive or carve-out method has been used in relation to those third party controls;

            b. for implementing the controls as designed; or

            c. for the operation of the controls as designed throughout the period;

        (v) to provide the assurance practitioner with:

            a. access to all information, such as records, documentation and other matters of which the responsible party is aware are relevant to the system and the controls within that system;

            b. additional information that the assurance practitioner may request from the responsible party for the purposes of the assurance engagement; and

            c. unrestricted access to persons within the entity from whom the assurance practitioner determines it necessary to obtain evidence;

[23] See ASAE 3000, paragraph 27.

(vi) if controls are designed to be operated by a third party, service or sub-service organisation, which may be material to the engagement, to obtain either:

a. a reasonable or limited assurance report, as appropriate, on the design and, if included in the scope of the engagement, the description of controls and/or implementation or operating effectiveness of controls, which covers the relevant controls at the third party; or

b. access to all information relevant to the design, description, implementation and/or operation of those controls, any additional information requested and access to persons from whom to obtain evidence at the third party.

25. The terms of engagement shall identify: (Ref: Para. A28-A36)

(a) the purpose of the engagement;

(b) whether the engagement is a reasonable or limited assurance engagement;

(c) whether the engagement is an attestation or direct engagement and, in the case of an attestation engagement, the form of the responsible party's or evaluator's evaluation of the controls or Statement and whether that Statement will be available to intended users or only referenced in the assurance report; (Ref: Para. A28)

(d) the subject matter of the engagement, including identification of the system and the component/s of control to be addressed and the functional and physical boundaries of that system and whether the subject matter includes description, implementation or operating effectiveness of controls, in addition to design; (Ref: Para. A29-A31, A34)

(e) the date or time period to be covered by the engagement; (Ref: Para. A32)

(f) if a third party operates controls on behalf of the entity which are integral to the system included in the scope of the assurance engagement, whether the inclusive or carve-out method has been used in relation to those third party controls;

(g) the criteria against which the design of controls will be assessed, expressed either as control objectives or as the overall objectives which those control objectives seek to address, including the source of those objectives or the party who is to provide or develop those objectives; (Ref: Para. A33-A34)

(h) the intended users of the assurance report;

(i) the content of the assurance report, including whether it will be a short-form or long-form report, including additional information such as the specific control objectives, the related controls, tests of controls conducted or detailed findings; and (Ref: Para. A35-A36)

(j) any other matters required by law or regulation to be included in the terms of engagement.

Acceptance of a Change in the Terms of the Engagement

26. If the engaging party requests a change in the terms of the engagement before the completion of the engagement, the assurance practitioner shall be satisfied that there is a reasonable justification for the change as required by ASAE 3000.[24] (Ref: Para. A26, A40-A41)

[24] See ASAE 3000, paragraph 29.

Assurance Report Prescribed by Law or Regulation

27. If law or regulation prescribes the criteria for evaluation of the relevant controls or the form and content of the assurance report, the assurance practitioner evaluates the criteria and form and content of the assurance report. If the criteria are unsuitable or if intended users might misunderstand the assurance report, the assurance practitioner shall:

    (a) not accept the engagement unless additional explanation in the report mitigates these circumstances; or

    (b) not include any reference within the assurance report to the engagement having been conducted in accordance with ASAE 3000 or this ASAE, if required to accept the engagement by law or regulation.

Quality Management

28. The assurance practitioner shall implement quality management procedures as required by ASAE 3000.[25]

Professional Scepticism, Professional Judgement and Assurance Skills and Techniques

29. The assurance practitioner shall apply professional scepticism, exercise professional judgement and apply assurance skills and techniques in planning and performing an assurance engagement on controls as required by ASAE 3000.[26] In applying professional scepticism, the assurance practitioner shall recognise the possibility that a deficiency in design, misstatement in the description of the system, deficiency in implementation or deviation in the operating effectiveness of controls due to fraud could exist, notwithstanding the assurance practitioner's past experience of the honesty and integrity of the entity's management and those charged with governance.

30. The assurance practitioner shall discuss with the engagement team how and where the entity's controls may be susceptible to circumvention due to fraud, including how fraud might occur. The discussion shall occur setting aside beliefs that the engagement team members may have that management and those charged with governance are honest and have integrity.

Planning and Performing the Engagement

Planning

31. The assurance practitioner shall plan the engagement so that it will be performed in an effective manner as required by ASAE 3000.[27] (Ref: Para. A42-A46)

32. In planning the engagement, if the scope of the engagement is based on overall control objectives, then the assurance practitioner shall identify, select or develop specific control objectives, to achieve the agreed overall control objectives against which the design of controls can be tested. If a description of the system is included in the scope of the engagement the specific control objectives are ordinarily included in that description. In an attestation engagement, if there is no description, the specific control objectives ordinarily are identified in documentation on which the responsible party's Statement is based. However, in a direct engagement, where the responsible party does not explicitly evaluate the controls for the purposes of the engagement or provide a Statement on the outcome of that evaluation, if there is no description, the assurance practitioner shall take a more active role in identifying, selecting or developing specific control objectives against which to evaluate the design of controls. (Ref: Para. A44-A45)

[25] See ASAE 3000, paragraphs 31-36.
[26] See ASAE 3000, paragraphs 37-39.
[27] See ASAE 3000, paragraph 40.

33. The assurance practitioner shall identify the controls relevant to the achievement of each specific control objective, which are either, identified in the terms of the engagement, or identified, selected or developed in planning the engagement under paragraph 32.

Materiality

34. The assurance practitioner shall consider materiality, as required by ASAE 3000,[28] when determining the nature, timing and extent of procedures.

35. The assurance practitioner shall identify a control or combination of controls as material if it is fundamental to the achievement of a control objective, included in the scope of the engagement, by mitigating the risks that threaten achievement of that objective. During the engagement the assurance practitioner shall reassess the materiality of the controls if matters come to their attention which indicate that the basis on which the materiality of those controls was determined has changed. (Ref: Para. A47-A52)

36. The assurance practitioner shall also consider materiality when evaluating the effect of accumulated deficiencies in the design, and if applicable, misstatements in the description of the system, deficiencies in implementation or deviations in operating effectiveness of controls as designed. Material deficiencies, misstatements and deviations are those which could reasonably be expected to influence relevant decisions of the intended users. (Ref: Para. A49-A50)

Obtaining an Understanding of the Entity's System and Other Engagement Circumstances and Identifying and Assessing Risks of Material Misstatement

37. The assurance practitioner shall obtain an understanding of the system, including controls, or the control components within the system that are included in the scope of the engagement, and other engagement circumstances, and on the basis of that understanding, the assurance practitioner shall: (Ref: Para. A53-A55)

    (a) for a direct engagement, consider whether the identification, selection or development of control objectives is appropriate, and/or select or develop further suitable control objectives; and

    (b) for both attestation and direct engagements:

        (i) identify the risks that threaten achievement of the control objectives;

        (ii) identify the controls designed to mitigate those risks;

        (iii) identify and assess the risk that: (Ref: Para. A56-A66)

            a. the controls are not suitably designed to achieve the control objectives identified;

            b. the description (if included in the scope of the engagement) does not fairly present the system as designed;

            c. the controls were not implemented (if included in the scope of the engagement) as designed; and

            d. the controls were not operating effectively (if included in the scope of the engagement) throughout the period; and

        (iv) identify the characteristics of the controls identified as a basis for designing assurance procedures to respond to the risks identified in paragraph 37(b)(iii).

[28] See ASAE 3000, paragraph 44.

38. When understanding the system within which the controls operate, the assurance practitioner shall consider other components of control beyond the components being reported upon, which may impact on the design, implementation or operating effectiveness of those controls. (Ref: Para. A67-A69)

Identifying Risks of Fraud

39. When performing risk assessment procedures and related activities to obtain an understanding of the system and other engagement circumstances, the assurance practitioner shall perform the following procedures, to obtain information for use in identifying the risks of the control objectives not being achieved due to fraud: (Ref: Para. A70)

    (a) make enquiries of management regarding:

        (i) management's assessment of the risk that controls may be circumvented due to fraud, including the nature, extent and frequency of such assessment;

        (ii) management's process for identifying and responding to the risks of fraud;

        (iii) management's communication, if any, to those charged with governance regarding its processes for identifying and responding to the risks of fraud; and

        (iv) management's communication, if any, to employees regarding its views on corrupt or fraudulent business practices and unethical behaviour;

    (b) make enquiries of those charged with governance, management, and others within the entity as appropriate, to determine whether they have knowledge of any actual, suspected or alleged fraud affecting the entity;

    (c) make enquiries of the internal audit function, where it exists, to determine whether it has knowledge of any actual, suspected or alleged fraud affecting the entity, and to obtain its views about the risks of fraud;

    (d) obtain an understanding of how those charged with governance exercise oversight of management's processes for identifying and responding to the risks of fraud in the entity and the internal control that management has established to mitigate these risks;

    (e) consider whether other information obtained by the assurance practitioner indicates risks of control objectives not being achieved due to fraud, for which mitigating controls are necessary;

    (f) evaluate whether the information obtained from the other risk assessment procedures and related activities performed indicates that one or more fraud risk factors are present; and

    (g) identify controls over matters for which decisions or actions are not routine, such as adjustments to records, development of estimates and activities outside the normal course of business.

Obtaining an Understanding of the Internal Audit Function

40. In planning the engagement, the assurance practitioner shall determine whether the entity has an internal audit function. If so the assurance practitioner shall obtain an understanding of the internal audit function and perform a preliminary assessment regarding: (Ref: Para. A71)

    (a) its impact on the system and the components of control within that system, including the control environment, risk assessment, information and communication, monitoring activities and control activities in relation to the system; and

(b) its effect on procedures to be performed by the assurance practitioner.

41. If the assurance practitioner plans to use the work of the internal audit function, in accordance with paragraph 40, the assurance practitioner shall evaluate it as required by ASAE 3000.[29] (Ref: Para. A72)

42. The use of internal auditors to provide direct assistance is prohibited in an assurance engagement conducted in accordance with this ASAE. Direct assistance is the performance of assurance procedures under the direction, supervision and review of the assurance practitioner.[30] This prohibition does not preclude reliance on the work of the internal audit function to modify the nature or timing, or reduce the extent, of assurance procedures to be performed directly by the assurance practitioner. (Ref: Para. A71)

Determining Whether and to What Extent to Use the Work of the Internal Audit Function

43. If the assurance practitioner's evaluation of the internal audit function confirms that the work of the internal audit function can be used for purposes of the engagement, then the assurance practitioner shall determine the planned effect of the work of the internal audit function on the nature, timing or extent of the assurance practitioner's procedures and in doing so, shall consider: (Ref: Para. A72)

(a) the nature and scope of work performed, or to be performed, on controls within the system by the internal audit function;

(b) the significance of that work to the assurance practitioner's conclusions; and

(c) the degree of subjectivity involved in the evaluation of the evidence obtained in support of those conclusions.

Documentation of the System

44. When obtaining an understanding of the system, if a description of the system is not prepared by the responsible party, the assurance practitioner shall document the system, to the extent considered appropriate as a basis for planning the engagement, which ordinarily includes identification of:

(a) the control objectives; and

(b) the controls designed to achieve those objectives.

Obtaining Evidence

45. Based on the assurance practitioner's understanding obtained under paragraph 37 the assurance practitioner shall perform assurance procedures to respond to assessed risks identified in paragraph 37(b)(iii) to obtain limited or reasonable assurance to support the assurance practitioner's conclusion. (Ref: Para. A73-A77)

46. The assurance practitioner shall design and perform additional procedures, the nature, timing and extent of which are responsive to the risks of material deficiency in the design, misstatement in the description, deficiency in the implementation or deviation in operating effectiveness of controls, having regard to the level of assurance required, reasonable or limited, as appropriate. (Ref: Para. A77)

[29] See ASAE 3000, paragraph 55.
[30] See ASAE 3000, paragraphs 3 and Aus 20.1.

Responses to Assessed Risks of Fraud

47. The assurance practitioner shall treat those assessed risks of control objectives not being achieved due to fraud as significant risks and accordingly, the assurance practitioner shall design and perform further assurance procedures, on controls designed to mitigate such risks, whose nature, timing and extent are responsive to those assessed risks, having regard to the level of assurance required, reasonable or limited, as appropriate.

Obtaining Evidence Regarding the Design of Controls

48. The assurance practitioner shall determine which of the controls at the entity are necessary to achieve the control objectives, whether those controls are presented in the entity's description of its system or identified by the assurance practitioner, and shall assess whether those controls were suitably designed. This determination shall include: (Ref: Para. A78-A84)

    (a) identifying the risks that threaten achievement of the control objectives;

    (b) evaluating whether the controls as designed would be sufficient to mitigate those risks when operating effectively, in all material respects; and

    (c) for engagements over a period, evaluating whether any changes in controls as designed during the period would be sufficient to mitigate those risks, in all material respects.

Limited Assurance	Reasonable Assurance
49L. In assessing the suitability of the design of controls, the assurance practitioner shall, at a minimum: (a) make enquiries of management or others within the entity regarding how the controls are designed to operate; and (b) examine the design specifications or documentation.	49R. In assessing the suitability of the design of controls, the assurance practitioner shall: (a) make enquiries of management or others within the entity regarding how the controls are designed to operate; (b) examine the design specifications or documentation; and (c) obtain an understanding of the control environment and consider other components of control, not included in the scope of the engagement, which may impact on the design of the specific controls included in the scope of the engagement. (Ref: Para. A67-A68, A85)
50L. If the assurance practitioner becomes aware of a matter(s) that causes the assurance practitioner to believe that a material deficiency in the design of controls may exist, the assurance practitioner shall design and perform additional assurance procedures until the assurance practitioner has obtained sufficient appropriate evidence to conclude on whether the design is suitable. The performance of such additional procedures shall not convert the engagement to a reasonable assurance engagement as they relate to the reduction of risk to an acceptable level with respect to that matter alone.	50R. In circumstances where the assurance practitioner obtains evidence which is inconsistent with the evidence on which the assurance practitioner originally based the assessment of the risk that the design of controls may be unsuitable, the assurance practitioner shall revise the assessment and modify the planned procedures accordingly.

Obtaining Evidence Regarding the Description

51. If the scope of the engagement includes assurance on the entity's description of the system, the assurance practitioner shall obtain and read that description, and shall evaluate whether those aspects of the description included in the scope of the engagement are fairly presented, including whether: (Ref: Para. A86)

    (a) the functions and services of the system are adequately identified;

    (b) the geographic, operational or functional boundaries of the system are appropriate in the circumstances of the engagement;

    (c) the date or time period covered by the description is appropriate;

    (d) the components of control covered by the description are appropriate for the scope of the engagement;

    (e) controls are described in sufficient detail to enable them to be identified for testing;

(f) in the case of a report covering operating effectiveness of controls, changes to the system or to controls during the period covered by the description are described adequately;

(g) the description does not omit or distort information relevant to the scope of the system or the controls being described;

(h) in the case of a service organisation, complementary user entity or client controls necessary to achieve the control objectives, are adequately described, including their importance in achieving the relevant objectives; (Ref: Para. A87)

(i) controls are described as designed and, if included in the scope of the engagement, as implemented; and

(j) functions outsourced to a third party or service organisation, if any, are adequately described, including whether the inclusive method or the carve-out method has been used in relation to them.

Limited Assurance	Reasonable Assurance
52L. The assurance practitioner shall determine whether the system has been described as designed and, if included in the scope of the engagement, as implemented, at a minimum through making enquiries. If the assurance practitioner determines that additional assurance procedures, such as inspection of records and documentation or observation of controls, are required to dispel or confirm a suspicion that a material misstatement in the description of the system exists, the performance of such additional procedures shall not convert the engagement to a reasonable assurance engagement as they relate to the reduction of risk to an acceptable level with respect to that matter alone. (Ref: Para.A87-A88))	52R. The assurance practitioner shall determine whether the system has been described as designed and, if included in the scope of the engagement, as implemented through other procedures in combination with enquiries. Those other procedures shall include inspection of records and other documentation evidencing the manner in which the system was designed, and if included in the scope of the engagement, observation of the controls which have been implemented. (Ref: Para. A87-A88)

Obtaining Evidence Regarding Implementation of Controls

53. If implementation is included in the scope of the engagement, the assurance practitioner shall obtain sufficient appropriate evidence that the controls identified as necessary to achieving the identified control objectives, were implemented as designed as at the specified date. Consequently, the assurance practitioner's evaluation of the design of controls often influences the nature, timing and extent of tests of implementation. (Ref: Para. A89-A90)

Limited Assurance	Reasonable Assurance
54L. The assurance procedures to test implementation of controls shall include, at a minimum, making enquiries and observation. If the assurance practitioner determines that additional assurance procedures, such as the inspection of records and documentation, are required	54R. The assurance procedures to test implementation of controls shall include enquiry of management or others within the entity and observation and/or inspection of records and other documentation, regarding the manner in which the controls were implemented.

Limited Assurance	Reasonable Assurance
to dispel or confirm a suspicion that a material deficiency in the implementation of controls exists, the performance of such additional procedures shall not convert the engagement to a reasonable assurance engagement as they relate to the reduction of risk to an acceptable level with respect to that matter alone.	Procedures may include determining: (Ref: Para. A90) (a) how any new or changes to existing systems were tested, installed and delivered to users; (b) who was allocated responsibility for operation, maintenance and monitoring of controls and system support; (c) the method of communication with and training of users; (d) the adequacy of system documentation, such as policies, manuals and instructions; (e) the adequacy of equipment, IT hardware, physical security and other infrastructure to enable the controls to operate effectively; (f) the sufficiency and suitability of human, physical and IT resources to maintain, operate, support and monitor controls implemented; (g) the existence of backup and contingency plans for control exceptions or breakdown; and (h) an appropriate means of selecting items for testing in order to meet the objectives of the procedure.

55. When designing and performing tests of implementation, the assurance practitioner shall determine whether controls implemented depend upon other controls (indirect controls) and, if so, whether it is necessary to obtain evidence supporting the implementation of those indirect controls.

Obtaining Evidence Regarding Operating Effectiveness of Controls

56. When reporting on operating effectiveness over the period, the assurance practitioner shall test those controls that the assurance practitioner has determined are necessary to achieve the control objectives identified, and assess their operating effectiveness throughout the period. Consequently, the assurance practitioner's evaluation of the design of controls often influences the nature, timing and extent of tests of operating effectiveness. Evidence obtained in prior engagements about the satisfactory operation of material controls in prior periods does not provide a basis for a reduction in testing of those controls, even if it is supplemented with evidence obtained during the current period. (Ref: Para. A91-A95, A104)

Limited Assurance	Reasonable Assurance
57L. The nature, timing and extent of tests of operating effectiveness, shall ordinarily be limited to discussion with entity personnel, observation of the system in operation and walk-through for an appropriate number of instances of material controls in operation to identify any deviations from the specified design. Alternatively, the results of exception reporting, monitoring or other management controls may be examined to provide evidence about the operation of the control rather than directly testing it. (Ref: Para. A94)	57R. The nature, timing and extent of tests of operating effectiveness, shall ordinarily include, in addition to discussion with entity personnel and observation of the system in operation for deviations from the specified design, re-performance of control procedures, or other examination and follow up of the application of controls, on a test basis to provide sufficient appropriate evidence on which to base an opinion. The results of exception reporting, monitoring or other management controls may be examined to reduce the extent of direct testing of the operation of the control but shall not eliminate it entirely. (Ref: Para. A94)
58L. The assurance practitioner shall apply professional judgement in determining the specific nature, timing and extent of procedures to be conducted, which will depend on the assessed risks of material deviations in the operating effectiveness of controls. If the assurance practitioner determines that additional assurance procedures are required to dispel or confirm a suspicion that a material deviation in the operating effectiveness of controls exists, the performance of such additional procedures shall not convert the engagement to a reasonable assurance engagement as they relate to the reduction of risk to an acceptable level with respect to that matter alone. (Ref: Para. A93, A101)	58R. The assurance practitioner shall apply professional judgement in determining the specific nature, timing and extent of procedures to be conducted, which will depend on the assessed risks of material deviations in the operating effectiveness of controls. (Ref: Para. A94-A95, A101)
	59R. When determining the extent of tests of controls, the assurance practitioner 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. Some controls operate continuously, while others operate only at particular times, so the tests of operating effectiveness shall be performed over a period of time that is adequate to determine that the control procedures are operating effectively. (Ref: Para. A95-A100, A102)

60. If a material control did not operate during the period, because the circumstances necessary to trigger that control did not arise, the assurance practitioner shall conclude that the controls, necessary to achieve the control objectives, operated effectively as designed if the assurance

practitioner obtained sufficient appropriate evidence that the circumstances necessary to trigger the control were adequately monitored by the entity and those circumstances did not arise during the period. (Ref: Para. A100)

61. Where control procedures have changed during the period subject to examination, the assurance practitioner shall test the operating effectiveness of both the superseded control(s) and the new control(s) and consider whether the new controls have been in place for a sufficient period to assess their effectiveness.

Sampling

62. When the assurance practitioner uses sampling to select controls for testing operating effectiveness over a period, the assurance practitioner shall: (Ref: Para. A102-A107)

    (a) consider the purpose of the procedure and the characteristics of the controls from which the sample will be drawn when designing the sample;

    (b) determine a sample size sufficient to reduce sampling risk to an acceptably low level;

    (c) select items for the sample in such a way that each sampling unit in the population has a chance of selection and the sample is representative of the population; and

    (d) if unable to apply the designed procedures, or suitable alternative procedures, to a selected item, treat that item as a deviation.

Evaluating the Evidence Obtained

63. ASAE 3000[31] requires the assurance practitioner to accumulate uncorrected misstatements identified during the engagement other than those that are clearly trivial. Misstatements in an engagement on controls include:

    (a) deficiencies in the suitability of the design of controls to achieve the control objectives;

    (b) misstatements in the description of the system;

    (c) deficiencies in the implementation of controls as designed; and

    (d) deviations in the operating effectiveness of controls as designed.

Deficiencies in Design of Controls

64. Where the assurance practitioner is unable to identify controls which are suitable or controls as designed are not suitable to achieve the identified control objective/s, this shall constitute a deficiency in the design of controls. The assurance practitioner shall accumulate deficiencies in the design of controls, other than those which are clearly trivial, and identify any compensating controls in the design which may mitigate those deficiencies in achieving the identified control objectives. The existence of compensating controls may be identified during the course of the engagement even if they were not identified in the design at the outset. The assurance practitioner shall assess the design deficiencies and determine whether they have a material impact on achieving the control objectives on which the assurance practitioner is required to conclude.

Misstatements in the Description of the System

65. If misstatements, such as insufficient detail to meet the needs of users or controls are described differently to the controls designed, are identified by the assurance practitioner in the

[31] See ASAE 3000, paragraph 51.

description of the system, the assurance practitioner shall advise the responsible party of those inaccuracies, inadequacies or omissions, other than those which are clearly trivial. The assurance practitioner shall provide the responsible party with the opportunity to amend the description, unless prohibited by legislation or the terms of the engagement, so that it reflects the system as designed at a point in time and/or during the period.

66. If the responsible party declines to amend the description when misstatements are identified, the assurance practitioner shall consider the materiality of the misstatements and their impact on the assurance conclusion. If the assurance conclusion is to be modified with respect to the fair presentation of the description of the system, the assurance practitioner shall consider whether the description can provide a basis for testing the design, implementation or operating effectiveness of the system.

Deficiencies in Implementation of Controls

67. The assurance practitioner shall accumulate any deficiencies in implementation of controls as designed, identified during the engagement, other than those which are clearly trivial, and assess whether the combined deficiencies will have a material impact on the implementation of controls as designed.

Deviations in Operating Effectiveness of Controls

68. The assurance practitioner shall investigate the nature and cause of any deviations from the design identified in the operation of the controls, other than those which are clearly trivial, and shall determine whether: (Ref: Para. A108-A109)

    (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 a reasonable or limited assurance conclusion, as applicable, that the control operated effectively throughout the period;

    (b) additional testing of the control or of other compensating or indirect controls is necessary to reach a reasonable or limited assurance conclusion, as applicable, on whether the controls relative to a particular control objective operated effectively throughout the period; or

    (c) the testing that has been performed provides an appropriate basis for a reasonable or limited assurance conclusion, as applicable, that the control/s did not operate effectively throughout the period.

69. In the extremely rare circumstances when the assurance practitioner considers a deviation discovered in a sample to be an anomaly and no other deviations have been identified that lead the assurance practitioner to conclude that the relevant control is not operating effectively throughout the period, the assurance practitioner shall obtain a high degree of certainty that such deviation is not representative of the population. The assurance practitioner shall obtain this degree of certainty by performing additional procedures to obtain sufficient appropriate evidence that the deviation is anomalous.

70. The assurance practitioner shall accumulate deviations in the operating effectiveness of controls identified during the engagement, other than those which are clearly trivial, and identify any compensating controls which may mitigate those deviations.

71. The assurance practitioner shall assess the impact of the combined control deviations and determine whether they will have a material impact on the operation of the system as designed in achieving the identified control objectives. (Ref: Para. A108-A109)

Indication of Fraud

72. If the assurance practitioner identifies a misstatement in the description, deficiency in the design or implementation of a control or a deviation in the operating effectiveness of that control, the assurance practitioner shall evaluate whether such a misstatement, deficiency or deviation is indicative of fraud. If there is such an indication, the assurance practitioner shall respond appropriately. (Ref: Para. A110)

73. If the assurance practitioner confirms that, the controls are not suitably designed, the description is materially misstated, the controls were not implemented as designed or did not operate effectively throughout the period or is unable to reach a conclusion, as a result of fraud the assurance practitioner shall modify the assurance conclusion accordingly.

Non-compliance with Laws or Regulations

74. If the assurance practitioner becomes aware of information concerning an instance of non-compliance or suspected non-compliance with respect to laws and regulations, whether due to the controls themselves not meeting compliance requirements or a failure of controls to prevent or detect non-compliance by the entity, the assurance practitioner shall:

    (a) discuss the matter with management and, if those matters are intentional or material, those charged with governance, unless management or those charged with governance are suspected of involvement in the non-compliance, in which case a level of authority above those suspected of involvement;

    (b) determine whether the assurance practitioner has a responsibility to report the identified or suspected non-compliance to parties outside of the entity and, if necessary, seek legal advice;

    (c) if sufficient information regarding suspected non-compliance cannot be obtained, evaluate the effect of insufficient evidence on the assurance report;

    (d) evaluate the implications of non-compliance in relation to other aspects of the engagement, including the risk assessment and the reliability of written representations; and

    (e) consider the impact on the assurance practitioner's conclusion of identified non-compliance.

Work Performed by an Assurance Practitioner's Expert

75. When the assurance practitioner plans to use the work of an assurance practitioner's expert, the assurance practitioner shall comply with the requirements in ASAE 3000.[32] (Ref: Para. A111)

Work Performed by Another Assurance Practitioner or a Responsible Party's or Evaluator's Expert

76. If the assurance practitioner plans to use information prepared using the work of another assurance practitioner or a responsible party's or evaluator's expert, as evidence, the assurance practitioner shall comply with the requirements of ASAE 3000.[33] (Ref: Para. A112-A113)

[32] See ASAE 3000, paragraph 52.
[33] See ASAE 3000, paragraphs 53-54.

Work Performed by the Internal Audit Function

Using the Work of the Internal Audit Function

77. In order for the assurance practitioner to use specific work of the internal audit function, the assurance practitioner shall determine its adequacy for the assurance practitioner's purposes in accordance with ASAE 3000.[34] In doing so, the assurance practitioner shall evaluate whether: (Ref: Para. A114)

    (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.

78. Although the assurance practitioner may consider the results of any tests of the operating effectiveness of controls conducted by the internal audit function when evaluating operating effectiveness, the assurance practitioner shall remain responsible for obtaining sufficient appropriate evidence to support the assurance practitioner's conclusion and, if appropriate, corroborate the results of such tests. When evaluating whether sufficient appropriate evidence has been obtained, the assurance practitioner shall consider that evidence obtained through direct personal knowledge, observation, re-performance and inspection is more persuasive than information obtained indirectly, from internal audit or from management or other entity personnel. Further, judgements about the sufficiency and appropriateness of evidence obtained and other factors affecting the assurance practitioner's conclusion, such as the materiality of identified control deficiencies or deviations, shall be those of the assurance practitioner. (Ref: Para. A114)

Effect on the Assurance Report

79. If the work of the internal audit function has been used, the assurance practitioner shall make no reference to that work in the section of the assurance report that contains the assurance practitioner's conclusion. (Ref: Para. A115)

Written Representations

80. The assurance practitioner shall request the responsible party, or other relevant person(s) within the entity, and any third party or service organisation(s), who are responsible for material controls for which the inclusive method has been used, to provide written representations, in addition to those required by ASAE 3000,[35] that the responsible party (or third party or service organisation, as applicable):

    (a) in the case of an attestation engagement, reaffirms their Statement regarding the outcome of the responsible party's evaluation of the controls against the control objectives with respect to the suitability of the design, and if included in the scope of the engagement, fair presentation of the description, implementation as designed

[34] See ASAE 3000, paragraph 55.
[35] See ASAE 3000, paragraph 56.

and/or operating effectiveness, at a point in time or throughout the period as appropriate;

(b) acknowledges its responsibility for establishing and maintaining the entity's system, including identifying the risks that threaten achievement of the identified control objectives, and designing, implementing and maintaining controls to mitigate those risks, including the risk of fraud, so that those risks will not prevent achievement of the control objectives and therefore that the identified control objectives will be achieved;

(c) has provided the assurance practitioner with all relevant information and access agreed to, as set out in paragraph 24(b)(v);

(d) has disclosed to the assurance practitioner any of the following of which it is aware may be relevant to the engagement:

(i) deficiencies in the design of controls to achieve the identified control objectives;

(ii) uncorrected misstatements, including omissions, in the description of the system;

(iii) deficiencies in the implementation of controls as designed;

(iv) instances where controls have not operated effectively as designed, including instances of non-compliance or suspected non-compliance with laws and regulations, fraud or suspected fraud;

(v) any events subsequent to the period covered by the assurance practitioner's report up to the date of the assurance report that could have a significant effect on the assurance practitioner's report; and

(vi) The identity of any third parties who operate controls on behalf of the entity, which form part of the system, and whether the carve-out method or inclusive method has been used in the description in relation to those controls and related control objectives.

81. The assurance practitioner shall evaluate written representations in accordance with ASAE 3000.[36] (Ref: Para. A116-A118)

Subsequent Events

82. Assurance procedures required to be conducted under ASAE 3000,[37] to identify all matters up to the date of the assurance report that may have caused the assurance practitioner to amend the assurance report on the design and/or description, implementation or operating effectiveness of controls, shall include enquiry as to whether the responsible party is aware of any events subsequent to the period covered by the assurance engagement up to the date of the assurance practitioner's report that may have caused the assurance practitioner to amend the assurance report. If the assurance practitioner is aware of such an event, remedial action is either not taken or is not effective in mitigating the impact on the assurance conclusion and information about that event is not disclosed by the responsible party, the assurance practitioner shall disclose the subsequent event in the assurance practitioner's report. If the event may impact the assurance conclusion, the assurance practitioner shall gather further evidence sufficient to determine whether the assurance conclusion remains appropriate or a modified assurance conclusion is required. (Ref: Para. A119-A123)

[36] See ASAE 3000, paragraphs 58-60.
[37] See ASAE 3000, paragraph 61.

Other Information

83. When any documents, that the assurance practitioner is aware of will contain the assurance practitioner's report on controls, also include other information, the assurance practitioner shall read that other information and respond to any material inconsistencies identified with the entity's system or an apparent misstatement of fact, in accordance with ASAE 3000.[38] (Ref: Para. A124-A126)

Forming the Assurance Conclusion

84. The assurance practitioner shall evaluate the sufficiency and appropriateness of the evidence obtained in the context of the engagement and, if necessary, attempt to obtain further evidence. If the assurance practitioner is unable to obtain necessary further evidence, the assurance practitioner shall consider the implications for the assurance practitioner's conclusion in accordance with ASAE 3000.[39] The assurance practitioner shall qualify their conclusion if the possible effects of undetected misstatements, deficiencies or deviations due to an inability to obtain sufficient appropriate evidence could be material, and shall disclaim their conclusion if the possible effects could be both material and pervasive.

85. When the assurance practitioner forms a conclusion in accordance with ASAE 3000,[40] the assurance practitioner shall evaluate the materiality, individually and in aggregate whether due to fraud or error, of any: (Ref: Para. A127)

    (a) deficiencies in the design of controls to achieve the identified control objectives;

    (b) uncorrected misstatements in the description of the system;

    (c) deficiencies in the implementation of controls as designed; and

    (d) deviations in the operating effectiveness of controls.

86. The assurance practitioner shall identify any compensating or indirect controls which may mitigate the deficiencies or deviations identified and impact on the evaluation of material deficiencies or deviations.

87. The assurance practitioner shall assess the impact of uncorrected deficiencies in the design, misstatements in the description, deficiencies in the implementation or deviations in operating effectiveness of controls, which are material individually or in combination, on the assurance practitioner's conclusion on the suitability of the design of the controls, and/or fair presentation of the description, implementation as designed or operating effectiveness of controls. If the deficiencies or deviations identified are: (Ref: Para. A127-A128)

    (a) material but not pervasive, the assurance practitioner shall qualify their assurance conclusion with respect to the relevant matter; or

    (b) material and pervasive, the assurance practitioner shall issue an adverse conclusion. If those material and pervasive deficiencies relate to the design, the assurance practitioner shall issue a modified report without performing any tests of operating effectiveness, as any conclusion on the operating effectiveness of controls based on an unsuitable design may be misleading.

[38] See ASAE 3000, paragraph 62.
[39] See ASAE 3000, paragraph 66.
[40] See ASAE 3000, paragraphs 64-65.

Preparing the Assurance Report

88. The assurance practitioner shall prepare the assurance report in accordance with ASAE 3000[41] for attestation engagements and shall also apply those requirements for direct engagements.

Assurance Report Content

89. For both attestation and direct engagements, the assurance practitioner shall include in the assurance report the basic elements required by ASAE 3000,[42] which are at a minimum: (Ref: Para. A139)

    (a) a title, indicating that it is an independent assurance report;

    (b) an addressee;

    (c) an identification of whether reasonable or limited assurance has been obtained by the assurance practitioner;

    (d) identification of the controls which comprise the underlying subject matter of the engagement including:

        (i) the distinguishing features of the system, boundaries of the system and the control components within that system which was subject to the assurance engagement;

        (ii) the date/s or period covered by the assurance engagement;

        (iii) the description of the system, if included in the scope of the engagement, and any parts of the description that are not covered by the assurance practitioner's conclusion;

        (iv) in the case of an attestation engagement, reference to the responsible party's Statement as required by paragraph 24(a)(i) and whether that Statement is available to intended users by accompanying the assurance report, reproduction in the assurance report or another identified source;

        (v) if functions relevant to the system of controls are performed by a third party:

            a. the nature of activities performed by the third party and whether the inclusive method or the carve-out method has been used in relation to the relevant controls operating at the third party;

            b. where the carve-out method has been used, a statement that the assurance engagement excludes the control objectives and related controls at relevant third parties, and that the assurance practitioner's procedures did not extend to controls at the third party; and

            c. where the inclusive method has been used, a statement that the assurance engagement includes control objectives and related controls at the third party, and that the assurance practitioner's procedures extended to controls at the third party.

    (e) identification of the overall and/or specific control objectives used as criteria for evaluating the design of controls and the party specifying those control objectives; (Ref: Para. A132)

[41] See ASAE 3000, paragraphs 67-69.
[42] See ASAE 3000, paragraph 69.

(f) if appropriate, a description of any significant inherent limitations associated with the evaluation of the design of the controls against the control objectives;

(g) when the control objectives are designed for a specific purpose, a statement alerting users to this fact and that, as a result, the description and/or responsible party's or evaluator's Statement may not be suitable for another purpose; (Ref: Para. A133-A134, A140)

(h) a statement that the responsible party or evaluator is responsible for:

  (i) in an attestation engagement:

    a. providing a Statement with respect to the outcome of the evaluation of the design against the identified control objectives, and, as applicable, the description, implementation and/or operating effectiveness of controls against the design;

    b. identifying the control objectives (where not identified by law or regulation, or another party, for example, a user group or a professional body); and

  (ii) in both an attestation and a direct engagement:

    a. the functions or services within the entity's system covered by the assurance practitioner's report;

    b. preparing the description of the entity's system, if included in the scope of the engagement, including the completeness, accuracy and method of presentation of that description; and

    c. designing and, if included in the scope of the engagement, implementing or operating effectively controls to achieve the control objectives relevant to the entity's system;

(i) a statement that the assurance practitioner's responsibility is to express a conclusion on the design of controls related to the overall and/or specific control objectives relevant to the entity's system, and, if included in the scope of the engagement:

  (i) the entity's description of the system;

  (ii) the implementation of the controls as designed; and/or

  (iii) the operating effectiveness of those controls;

(j) a statement that the engagement was performed in accordance with ASAE 3150 *Assurance Engagements on Controls*;

(k) a statement that the firm of which the assurance practitioner is a member applies ASQM 1 or other professional requirements, or requirements in law or regulation, that are at least as demanding as ASQM 1. If the assurance practitioner is not a professional accountant, the statement shall identify the professional requirements, or requirements in law or regulation, applied that are at least as demanding as ASQM 1;

(l) a statement that the assurance practitioner complies with the independence and other relevant ethical requirements related to assurance engagements, or other professional requirements, or requirements imposed by law or regulation, that are at least as demanding;

(m) a summary of the work performed by the assurance practitioner to obtain reasonable or limited assurance and a statement of the assurance practitioner's belief that the

evidence obtained is sufficient and appropriate to provide a basis for the assurance practitioner's conclusion, and, if applicable, a statement that the assurance practitioner has not performed any procedures regarding the implementation or operating effectiveness of controls and therefore no conclusion is expressed thereon. In the case of a limited assurance engagement, in which an appreciation of the nature, timing, and extent of procedures performed is essential to understanding the assurance practitioner's conclusion, the summary of the work performed shall state that:
(Ref: Para. A135-A138)

(i) the procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement; and

(ii) consequently, the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed;

(n) a statement of the limitations of controls and, if applicable, of the risk of projecting to other periods the outcome of any evaluation of the operating effectiveness of controls;
(Ref: Para. A129)

(o) either, the assurance practitioner's opinion for a reasonable assurance engagement or the assurance practitioner's conclusion for a limited assurance engagement about whether, in all material respects:

(i) for a report on design of controls:

a. the controls were suitably designed to achieve the identified control objectives; and

b. if included in the scope of the engagement, the description fairly presents the system as designed;

as at a specified date;

(ii) for a report on design and implementation of controls:

a. the controls were suitably designed to achieve the identified control objectives;

b. if included in the scope of the engagement, the description fairly presents the system as designed; and

c. the controls, necessary to achieve the control objectives, were implemented as designed;

as at a specified date;

(iii) for a report on design and operating effectiveness of controls:

a. the controls were suitably designed to achieve the identified control objectives;

b. if included in the scope of the engagement, the description fairly presents the system as designed; and

c. the controls, necessary to achieve the control objectives, operated effectively as designed;

throughout the period;

(iv) when the assurance practitioner expresses a modified conclusion, the assurance report shall contain:

a. a section (entitled: Basis for Qualified/Adverse/Disclaimer of Conclusion/Opinion) that provides a description of the matter(s) giving rise to the modification; and

b. a section that contains the assurance practitioner's modified conclusion;

(l) the assurance practitioner's signature, the date of the assurance report and the location in the jurisdiction where the assurance practitioner practices.

90. If the assurance practitioner is required to provide a long-form assurance report to meet the information needs of users, as agreed in the terms of engagement, or as required by law or regulation, the assurance practitioner's report shall include a separate section, or an attachment, containing any other information and explanations that are not intended to affect the assurance practitioner's conclusion and are clearly identified as such. (Ref: Para. A130-A131)

91. If the assurance practitioner is required to conclude on other subject matters under different AUASB standards in conjunction with an engagement to report under this ASAE, the assurance report shall include a separate section for each subject matter in the assurance report, clearly differentiated by appropriate section headings.

Emphasis of Matter and Other Matter Paragraphs

92. The assurance practitioner shall include an Emphasis of Matter or Other Matter paragraph in the circumstances provided for in ASAE 3000[43] for an attestation engagement. In a direct engagement, if the assurance practitioner considers it necessary to communicate a matter that, in the assurance practitioner's judgement, is relevant to intended users' understanding of the engagement, the assurance practitioner's responsibilities or the assurance report, the assurance practitioner shall include in the assurance report an Other Matter paragraph, with an appropriate heading, that clearly indicates the assurance practitioner's conclusion is not modified in respect of the matter. (Ref: Para. A122-A123, A149)

Modified Conclusions

93. If the assurance practitioner concludes that:

(a) the controls were not suitably designed to achieve the control objectives, in all material respects;

(b) the entity's description does not fairly present, in all material respects, the system as designed;

(c) the controls were not implemented as designed, in all material respects;

(d) the controls tested, which were those necessary to achieve the control objectives, did not operate effectively, in all material respects throughout the period; or

(e) the assurance practitioner is unable to obtain sufficient appropriate evidence;

the assurance practitioner's conclusion shall be modified, and the assurance practitioner's report shall include a section with a clear description of all the reasons for the modification. (Ref: Para. A141-A148)

[43] See ASAE 3000, paragraph 73.

Scope Limitation

94. A limitation on the scope of the assurance practitioner's work may be imposed by the terms of the engagement or by the circumstances of the particular engagement. When the limitation is imposed by the terms of the engagement, and the assurance practitioner believes that an inability to form an opinion or reach a conclusion would need to be expressed, the engagement shall not be accepted or continued past the current period, unless required to do so by law or regulation.

95. When a scope limitation is imposed by the circumstances of the particular engagement, the assurance practitioner shall attempt to perform alternative procedures to overcome the limitation. When a scope limitation exists and remains unresolved, the wording of the assurance practitioner's conclusion shall indicate that it is qualified as to the effects of any evidence that the controls are not suitably designed, the description is not fairly presented, the controls are not implemented as designed or not operating effectively, which might have been identified had the limitation not existed. If the effect of the unresolved scope limitation is both material and pervasive, the assurance practitioner shall express a disclaimer of conclusion. (Ref: Para. A148)

Other Communication Responsibilities

96. The assurance practitioner shall consider whether, pursuant to the terms of the engagement and other engagement circumstances, any matter has come to the attention of the assurance practitioner that is to be communicated with the responsible party, the evaluator, the engaging party, those charged with governance or others, as required by ASAE 3000.[44] If during the course of the engagement the assurance practitioner identifies any control design deficiencies, deficiencies in implementation or deviations in operating effectiveness, other than those which are clearly trivial, the assurance practitioner shall report to an appropriate level of management or those charged with governance on a timely basis those control deficiencies or deviations. (Ref: Para. A149-A150)

97. If the assurance practitioner has identified a fraud or has obtained information that indicates that a fraud may exist, the assurance practitioner shall communicate these matters on a timely basis to the appropriate level of management or those charged with governance in order to inform those with primary responsibility for the prevention and detection of fraud of matters relevant to their responsibilities. The assurance practitioner shall determine whether there is a responsibility to report the occurrence or suspicion to a party outside the entity. (Ref: Para. A150)

98. The assurance practitioner shall design engagement procedures to gather sufficient appropriate evidence to form a conclusion in accordance with the terms of the engagement. In the absence of a specific requirement in the terms of engagement the assurance practitioner does not have a responsibility to design procedures to identify matters outside the scope of the engagement that may be appropriate to report to management or those charged with governance.

Documentation

99. The assurance practitioner shall prepare documentation in accordance with ASAE 3000.[45] In documenting the nature, timing and extent of procedures performed as required by ASAE 3000, the assurance practitioner shall record: (Ref: Para. A151)

    (a) the identifying characteristics of the controls being tested;

    (b) who performed the work and the date such work was completed; and

[44] See ASAE 3000, paragraph 78.
[45] See ASAE 3000, paragraphs 79-83.

(c) who reviewed the work performed and the date and extent of such review.

100. If the assurance practitioner uses specific work of the internal audit function, the assurance practitioner shall document the conclusions reached regarding the evaluation of the adequacy of the work of the internal audit function, and the procedures performed by the assurance practitioner on that work.

* * *

Application and Other Explanatory Material

Application (Ref: Para. 1)

A1. Engagements which are not covered by this ASAE include financial reporting controls at a service organisation which are reported under ASAE 3402, including reasonable assurance reports on internal controls of Investor-directed portfolio services (IDPS) and IDPS-like services relating to specific annual investor statements as required by ASIC Class Orders.[46] These service auditor's reports may be used as evidence for the financial audit of a user entity under ASA 402.[47]

Introduction (Ref: Para. 3-14, Appendix 2)

A2. The primary purpose of an assurance engagement is the conduct of assurance procedures to provide an assurance conclusion. However, the assurance practitioner is not precluded from providing recommendations for improvements to controls in conjunction with or as a result of conducting an assurance engagement to report on controls.

A3. The risks, control objectives and related controls addressed in an engagement under this ASAE may relate to any subject matter relevant to the entity. The subject matter can be any activity of the entity, whether a function or service, such as: compliance with legislation or regulation; financial reporting; management reporting; emissions and energy reporting; economy, efficiency and effectiveness or ethical conduct.

A4. Controls are put in place by an entity to reduce to an acceptably low level the risks that threaten achievement of the entity's control objectives. To implement effective controls, the entity needs to:

(a) identify or develop control objectives;

(b) identify the risks that threaten achievement of those control objectives;

(c) design and implement controls that would mitigate those risks, in all material respects, when operating effectively; and

(d) monitor the operation of those controls to determine whether they are operating effectively throughout the period.

A5. Assurance engagements on controls are structured to suit the particular circumstances of the engagement and the needs of users, for example:

- Reports for internal use to assess whether the controls designed will achieve identified control objectives prior to implementation, may be restricted use reports on design and description of controls over a specific system or a report on design only in long-form, so that the controls as designed can be clearly identified.
- Reports for internal use to determine whether the implementation of new controls or controls within a new system was carried out satisfactorily as designed so that the controls are able to operate effectively, may be restricted use reports on design, description and implementation of controls or design and implementation in long-form if no description is available.
- Publicly available reports, such as a report for customers of cloud services to provide assurance with respect to IT security, including confidentiality, integrity and availability of IT resources relating to the services provided, presented in the short-

[46] See CO 13/763 *Investor directed portfolio services* and CO 13/762 *Investor directed portfolio services provided though a registered managed investment scheme.*
[47] See ASA 402 *Audit Considerations Relating to an Entity Using a Service Organisation.*

form only, on design and operating effectiveness. Long-form reports may contain competitively sensitive information or information which undermines security as a result of the detailed description of tests of controls and deficiencies detected and may not be suitable for wide distribution.

- Reports on service organisation's controls relevant to the security, availability, processing integrity, confidentiality or privacy of the information processed or stored for user entities in order for the user entity to be able to assess and manage the risks associated with outsourcing services provided to customers, will usually require a long-form restricted use report on design, description and operating effectiveness of controls, detailing the tests conducted and the results of those tests. The services provided by service organisations in these circumstances may include: cloud computing, managed IT security, customer on-line or telephonic support, sales force automation (order processing, information sharing, order tracking, contact management, customer management, sales forecast analysis or employee performance evaluation), health care or insurance claim management and processing or IT outsourcing services.

A6. The primary practical difference for the assurance practitioner between an attestation and a direct engagement is the additional work effort for a direct engagement when planning the engagement and understanding the system and other engagement circumstances. In a direct engagement the assurance practitioner identifies, selects or develops the control objectives which address the purpose or overall objectives of the engagement and identifies the controls which are designed to achieve those objectives. This difference affects the assurance practitioner's work effort in planning a direct engagement if the controls relevant to the control objectives have not been identified or documented and in understanding the entity's system where a description of the system is not available.

A7. In a three party relationship, which is an element of an assurance engagement,[48] the responsible party may or may not be the engaging party, but is responsible for the controls which are the subject matter of the engagement and is a separate party from the intended users. The responsible party and the intended users may both be internal to the entity, for example if the responsible party is at an operational level of management and the intended users are at the level of those charged with governance, such as the Board or Audit Committee. See Appendix 2 for a discussion of how each of these roles relate to an assurance engagement on controls.

Relationship with ASAE 3000, Other Pronouncements and Other Requirements (Ref: Para. 9-14)

A8. Although, this ASAE does not apply to engagements on controls required to be conducted under ASAE 3402, an engagement may include combined reporting under this ASAE and ASAE 3402. A service organisation may agree by contractual arrangements with user entities to provide an assurance report on controls for the purposes of both providing evidence for user entities' financial report audit and to satisfy user entities' obligations to customers or employees. Consequently, the assurance report may contain a section prepared under ASAE 3402 which concludes on the operating effectiveness of controls at the service organisation that are likely to be relevant to user entities' internal control as it relates to financial reporting and a section prepared under this ASAE which concludes on controls relevant to user entities' operational needs, such as accessibility and availability of IT resources, or contractual commitments to customers or employees, such as security, confidentiality and privacy of personal information or health and safety of workers engaged to produce products supplied.

[48] See *Framework for Assurance Engagements.*

Definitions (Ref: Para. 17(f))

A9. Components of control are defined by the control framework applied. For example the components of control may comprise:

(a) the COSO Framework components: the control environment, risk assessment, control activities, information and communication and monitoring activities;

(b) COBIT 5, framework for the governance and management of enterprise IT, enablers: principles, policies and frameworks; processes; organisational structures; culture, ethics and behaviour; information; services, infrastructure and applications; and people, skills and competencies;

(c) IT-enabled systems components:

(i) infrastructure – physical facilities, equipment, IT hardware and IT networks;

(ii) software – IT operating system, software applications and utilities;

(iii) people – IT developers, testing and implementation personnel, system and database administrators, operators, users and managers;

(iv) procedures – automated and manual procedures involved in the system's operation; and

(v) data – information processed, generated, stored, transmitted and managed, including transactions, files, messages, images, records, databases and tables.

Ethical Requirements (Ref: Para. 19)

A10. In accepting an assurance engagement on controls, the assurance practitioner, in order to comply with relevant ethical requirements, considers whether the assurance practitioner has provided internal audit or consulting services with respect to the design or implementation of controls at the entity, as any such past or current engagements are likely to impact on the assurance practitioner's independence and are likely to preclude acceptance of the engagement.

Acceptance and Continuance (Ref: Para. 20-27)

Preconditions for the Assurance Engagement (Ref: Para. 20)

A11. In a direct engagement, in order to establish whether the preconditions for an assurance engagement are present as required by ASAE 3000, circumstances may require the assurance practitioner to commence the assurance engagement to obtain information that the preconditions can be satisfied. If the assurance practitioner develops the control objectives for evaluating the design of controls, the assurance practitioner may not be able to determine if suitable criteria will be available until after the assurance engagement has commenced.

Competence and Capabilities to Perform the Engagement

A12. Relevant competence and capabilities, including having sufficient time to perform the controls engagement, as required by ASAE 3000[49] by persons who are to perform the engagement, include matters such as the following:

[49] See ASAE 3000, paragraph 32.

- Knowledge of the relevant industry, controls framework, type of system and of the nature of the overall objective of the relevant controls (for example: financial reporting, emissions quantification or regulatory compliance).
- An understanding of IT and systems.
- Experience in evaluating risks as they relate to the suitable design of controls.
- Experience in the design and execution of tests of controls and the evaluation of the results.

Rational Purpose

A13. When deciding whether to accept an engagement to report on the design, but not implementation of controls, or design and implementation of controls at a point in time, but not the operating effectiveness of controls over the period, the assurance practitioner considers whether the engagement has a rational purpose, as required when meeting the preconditions of an assurance engagement in accordance with ASAE 3000.[50] An engagement on design only, may have a rational purpose if the controls designed have neither been implemented, nor are in operation. However, if the design has already been implemented or is in operation, then the assurance practitioner considers whether the purpose of the engagement is logical or if the assurance report may be misleading to users. For an engagement on design and implementation, if the controls are in operation, the assurance practitioner considers whether the assurance report is likely to meet the needs of users or may be misunderstood as providing assurance on operating effectiveness of controls. Nevertheless, it may be justifiable for the entity to seek assurance on the design of new controls prior to implementation or assurance on design and implementation of a change in controls, even if there are existing controls in operation.

A14. When considering the acceptance of a limited assurance engagement on controls, ASAE 3000 requires the assurance practitioner to determine whether a meaningful level of assurance is expected to be able to be obtained,[50] which may include whether a limited assurance engagement is likely to be meaningful to users. In making this assessment, the assurance practitioner considers the intended users of the assurance report and whether they are likely to understand the limitations of a limited assurance engagement, including the need to read the assurance report in detail to understand the assurance procedures performed and the assurance obtained.

Assessing the Appropriateness of the Subject Matter (Ref: Para. 21, Appendix 1, Appendix 2)

A15. The controls which are the subject matter of the engagement may be defined by:

(a) the component/s of control which they address, which are determined by the control framework applied, but may include:

(i) the control environment;

(ii) risk assessment;

(iii) control activities;

(iv) information and communication; or

(v) monitoring activities;

(b) the system, being the function or service provided by that system; and

[50] See ASAE 3000, paragraph 24(b)(vi).

(c) the entity or facility boundaries.

Assessing the Suitability of the Criteria (Ref: Para. 22-23, Appendix 1, Appendix 2*)*

A16. Control objectives ordinarily comprise the main criteria for evaluation of the design of controls. In assessing the suitability of the criteria for evaluating the design of controls, the assurance practitioner considers whether the control objectives:

- Are specified by outside parties, such as a regulatory authority, a user group, or a professional body that follows a transparent due process, identified by the entity or identified by the assurance practitioner themselves.
- Address compliance requirements, specified by legislation, regulation or by contractual agreement.
- If identified by the entity, are complete and address each of the overall objectives relevant to the system, whether a function or service.

A17. Additional criteria for assessing the suitability of the design may be derived from the risks that threaten achievement of the control objectives identified.

A18. In a direct engagement, the assurance practitioner may not be provided with control objectives and so will need to identify, select or develop the control objectives to apply as the criteria for evaluating the design of controls. The assurance practitioner may either identify or select control objectives which have already been developed or develop the control objectives themselves. The work effort required by the assurance practitioner, when planning a direct engagement, in identifying suitable controls objectives as well as the related controls, is ordinarily substantially greater than for the equivalent attestation engagement.

A19. The responsible party implicitly or explicitly makes assertions regarding the recognition, measurement, presentation, disclosure or compliance of the subject matter, which reflect the overall objectives of the system. These overall objectives can be applied in assessing the suitability of the specific control objectives to meet the needs of users. Overall objectives may be expressed in different terms under different frameworks, such as "key system attributes", "goals" or "business requirements", and may include:

(a) for transactions, activities and events over a period:

(i) occurrence;

(ii) completeness;

(iii) accuracy;

(iv) cut-off and

(v) classification.

(b) for volumes, amounts or balances as at a date:

(i) existence;

(ii) rights and obligations;

(iii) completeness; and

(iv) valuation and allocation.

(c) for presentation and disclosure in a report:

(i) occurrence and rights and obligations;

(ii) completeness;

(iii) classification and understandability;

(iv) accuracy and valuation; and

(v) consistency.

(d) for performance of the system:

(i) economy;

(ii) efficiency; and

(iii) effectiveness.

(e) for contractual obligations of a service organisation, providing IT, on-line or cloud services for virtual processing of information, communications or data and storage of data or information, over a period:[51]

(i) security;

(ii) confidentiality;

(iii) privacy;

(iv) accessibility and availability; and

(v) data integrity, including:

a. completeness;

b. accuracy;

c. timeliness; and

d. authorisation.

A20. The way in which the overall objectives, described above, are expressed will vary widely depending on the control framework applied or developed. For example COBIT 5 categorises "goals" for Enterprise IT as: intrinsic quality, contextual quality and access and security. APRA Prudential Practice Guide PPG 234 *Management of security risk in information and information technology* (1 February 2010) defines "security risk" as the potential compromise to: confidentiality (authorised access), integrity (completeness, accuracy and freedom from unauthorised change) and availability (accessibility and usability). The responsible party may apply whichever control framework is either, required by regulation or legislation, or, for a voluntary engagement, which represents suitable criteria for the evaluation of controls in the particular circumstances of the engagement.

A21. In assessing the control objectives as suitable criteria for design of controls, if the scope of the engagement specifies overall control objectives then suitable criteria are specific control objectives which address each of those overall objectives.

A22. Suitable criteria need to be identified by the parties to the engagement and agreed by the engaging party and the assurance practitioner. The assurance practitioner may need to discuss

[51] The materiality matrix in Appendix 4 plots these overall objectives to provide a frame of reference for assessing materiality.

the criteria to be used with those charged with governance, management and the intended users of the report. Criteria can be either established or specifically developed. The assurance practitioner normally concludes that established criteria embodied in laws or regulations or issued by professional bodies, associations or other recognised authorities that follow due process are suitable when the criteria are consistent with the objective. Other criteria may be agreed to by the intended users of the assurance practitioner's report, or a party entitled to act on their behalf, and may also be specifically developed for the engagement.

A23. In situations where the criteria have been specifically developed for the engagement, including where the assurance practitioner develops or assists in developing suitable criteria, the assurance practitioner obtains from the intended users or a party entitled to act on their behalf, acknowledgment that the specifically developed criteria are sufficient for the user's purposes.

A24. Additional criteria that the assurance practitioner may consider when evaluating a description include, whether the description presents:

(a) the types of services provided, including, as appropriate, the nature of the data stored and/or information processed;

(b) the procedures by which data was recorded and stored and information was processed;

(c) how the system dealt with significant events and conditions;

(d) The process used to prepare reports for clients;

(e) relevant control objectives and controls designed to achieve those objectives;

(f) controls that the entity assumed, in the design of the system, would be implemented by clients, and which, if necessary to achieve control objectives, are identified in the description along with the specific control objectives that cannot be achieved by the entity alone;

(g) aspects of other components of control that are relevant to the system described;

(h) if the scope of the engagement is over a period, relevant details of changes to the system during the period; and

(i) information relevant to the scope of the system being described without distortion or omission, while acknowledging that the description is prepared to meet the needs of the identified users and may not, therefore, include every aspect of the system that each user may consider important in its own particular environment.

A25. In assessing the suitability of the design of the controls as criteria for evaluating implementation of controls, the assurance practitioner may consider if the design encompasses:

(a) the extent of documentation, including manuals, instructions and policies, needed by those applying the controls to operate or monitor the controls as designed;

(b) the allocation of responsibilities for controls to enable the controls to be carried out;

(c) the method of communication with and training of those applying the controls sufficient for them to carry out manual controls so they operate as designed; and

(d) for IT enabled systems, an implementation plan for:

(i) the development, acquisition or outsourcing of IT systems, data storage, hardware and other infrastructure needed to meet the specifications required by the design of the controls; and

(ii) the testing and delivery of IT systems sufficient to enable the IT controls to operate as designed.

A26. The criteria may need to be amended during the engagement, if for example more information becomes available or the circumstances of the entity change. Any changes in the criteria are discussed with the engaging party and, if appropriate the intended users.

Agreeing on the Terms of the Engagement (Ref: Para. 24-25, Appendix 1, Appendix 5)

A27. Even if the responsible party is not a party to the terms of the engagement, the assurance practitioner may seek to obtain the responsible party's written agreement regarding their responsibilities as set out in paragraph 24, if practicable.

A28. When agreeing whether the engagement is to be conducted as an attestation or direct engagement, the assurance practitioner considers factors such as whether:

(a) there is a regulatory requirement or users need an evaluation of the subject matter by the responsible party or evaluator;

(b) the entity has the resources and expertise to prepare a suitable description or documentation of the controls objectives and related controls and conduct a meaningful evaluation of those controls; or

(c) it is more cost effective for the entity to identify the specific control objectives and related controls, evaluate those controls as the basis for an attestation engagement, rather than it being necessary for the assurance practitioner to do so in a direct engagement.

A29. When identifying the subject matter in the terms of engagement, the system is clearly defined. If the scope of the engagement is imposed by legislation, regulation or other requirement and does not explicitly include design, design is still implicit in the assurance practitioner's conclusion on description, implementation or operating effectiveness of controls and the work undertaken will include evaluation of the suitability of the design to achieve the control objectives. If the controls are specified by regulation and there is no scope for the assurance practitioner to evaluate the design of those controls, then the assurance practitioner conducts the engagement as a compliance engagement under ASAE 3100.[52]

A30. The subject matter of an engagement conducted under this ASAE is controls which may be directed at a broad range of objectives of the entity. Categories of objectives may be defined by the control framework applied and may include: operations, reporting or compliance objectives. Operations may include performance objectives aimed at economy, efficiency and effectiveness. Reporting objectives may address financial reporting, management reporting or emissions and energy reporting. Compliance objectives may address regulatory, legislative, industry or contractual requirements.

A31. The subject matter may be restricted to a system within the boundaries of the entity, location or operational facility.

A32. The assurance practitioner considers the needs of users in agreeing the point in time or period to be covered by the assurance engagement, so that the report is not likely to be misleading.

A33. If the criteria are control objectives which are available when agreeing the terms of engagement, they may be listed or attached to the engagement letter or other written terms. Otherwise the criteria may be expressed as overall objectives which may be broken down into detailed objectives as part of the engagement.

[52] See ASAE 3100 *Compliance Engagements.*

A34. Whether the assurance practitioner is required to conclude on the design, description, implementation and/or operating effectiveness of controls in achieving overall objectives or specific control objectives will have a significant impact on the work effort required to reach a conclusion. Whether the criteria against which the assurance practitioner assesses controls are the overall control objectives or specific control objectives is determined when accepting the engagement and will depend on the information needs of users. If the conclusion is centred on achievement of overall objectives, then the assurance practitioner can focus the work effort on controls which are material to achieving those overall objectives. In contrast if the assurance report is required to conclude on each specific control objective and/or identified controls to achieve those objectives, then it will be necessary for the assurance practitioner to gather evidence in relation to each individual control objective and/or control identified so that the assurance practitioner can conclude at that level of detail. This is depicted in the table below.

Conclusion expressed on:	Overall Control Objectives	Specific Control Objectives	Control Procedures
Materiality based on:	Impact on Overall Control Objectives	Impact on Specific Control Objectives	Impact on each Control Procedure
Controls tested:	Controls necessary to mitigate the risks threatening overall objectives	Controls necessary to mitigate the risks threatening specific objectives	Control procedures

A35. When agreeing whether the report will be in long-form, including matters such as tests of controls and detailed findings, the assurance practitioner considers both the needs of users and the risks of users misunderstanding the context of the procedures conducted or the findings reported. A long-form report may be necessary for users whose assurance providers intend to use specific findings as evidence for an assurance engagement with respect to the user entity or to meet the information needs of a regulator. Reporting tests of controls and findings may be appropriate where the users are knowledgeable with respect to assurance and controls and, therefore, not likely to misinterpret those findings.

A36. Example engagement letters are contained in Appendix 5.

Reasonable Basis for Responsible Party's Statement (Ref: Para. 24(a)(ii), Appendix 7 Example 1)

A37. If the assurance practitioner is engaged to report on the operating effectiveness of controls this fact is not a substitute for the responsible party's own processes to provide a reasonable basis for its Statement on the outcome of the evaluation of controls. If the responsible party's Statement claims that the controls related to the control objectives operated effectively throughout the period, this Statement may be based on the entity's monitoring activities. Monitoring of controls is itself a component of control and 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 deficiencies to appropriate individuals within the entity, and taking necessary corrective actions. The entity 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 an entity and include regular management and supervisory activities. Internal auditors or personnel performing similar functions may contribute to the monitoring of an entity'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.

A38. In order for an engagement to be conducted as an attestation engagement, the responsible party needs to be able to identify:

(a) the specific control objectives which address each overall control objective;

(b) the controls designed to achieve each of the specific control objectives; and

(c) the basis for the responsible party's evaluation of the design, and/or implementation or operating effectiveness of controls, including documentation supporting the outcome of that evaluation.

If the responsible party cannot demonstrate that they have an adequate basis for their evaluation of controls, as reflected in the responsible party's Statement, then the assurance practitioner may decide not to accept the engagement as an attestation engagement, but may accept the engagement as a direct engagement, if appropriate.

A39. The adequacy of the basis for the responsible party's evaluation of the controls reflected in the responsible party's Statement, including appropriate documentation, will impact the assurance practitioner's risk assessment. An example of a Statement is contained in Appendix 7, example 1.

Acceptance of a Change in the Terms of the Engagement (Ref: Para. 26)

A40. 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 assurance practitioner's conclusion would be modified or to reduce the level of assurance to be obtained from reasonable to limited due to a limitation in the available evidence.

A41. 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 an outsourced activity when the entity cannot arrange for access by the assurance practitioner, and the method used for dealing with the services provided by that outsourced activity is changed from the inclusive method to the carve-out method.

Planning and Performing the Engagement

Planning (Ref: Para. 31-33*)*

A42. When developing the engagement plan, the assurance practitioner considers factors such as:

(a) matters affecting the industry in which the entity operates, for example economic conditions, laws and regulations, and technology;

(b) risks to which the entity is exposed that are relevant to the system being examined;

(c) the quality of the control environment within the entity and the role of the governing body, audit committee and internal audit function;

(d) knowledge of the entity's internal control structure obtained during other engagements;

(e) the extent of recent changes if any, in the entity, its operations or its internal control structure;

(f) methods adopted by management to evaluate the effectiveness of the internal control structure;

(g) preliminary judgements about significant risk;

(h) the nature and extent of evidence likely to be available;

(i) the nature of control procedures relevant to the subject matter and their relationship to the internal control structure taken as a whole; and

(j) the assurance practitioner's preliminary judgement about the effectiveness of the internal control structure taken as a whole and of the control procedures within the system.

A43. In engagements for which a description of the system is not provided to the assurance practitioner, the assurance practitioner, in planning the engagement, identifies the controls in place through procedures such as enquiry, observation or examination of records or documentation. The assurance practitioner may do this in conjunction with evaluating the suitability of the design of controls to achieve the control objectives and these procedures may also provide evidence of the implementation or operating effectiveness of controls.

A44. In a direct engagement, the responsible party is not required to identify specific control objectives, or evaluate whether controls are suitably designed to achieve those objectives and, if applicable, the description is fairly presented, the controls were implemented as designed or operating effectively. Consequently, in planning a direct engagement the assurance practitioner considers the additional work required to identify specific control objectives and related controls and any increased risk of deficiencies in the design of controls compared to an equivalent attestation engagement.

A45. The process necessary to identify the overall control objectives, specific control objectives and controls relevant to the achievement of those objectives, will vary depending on the size and complexity of the entity or component which is being assured. In identifying, selecting or developing suitable control objectives, the assurance practitioner considers relevant regulation, industry or other requirements and which control objectives are likely to address users' needs. Whilst the assurance practitioner needs to assess which controls are necessary to achieve the control objectives which they will be concluding upon as a basis for determining which controls to test, it does not necessarily need to be a complex process for a small entity or component. The manner in which the identification of control objectives and related controls is documented may range from a simple reference to a more complex matrix. An understanding of whether a control is relevant to the achievement of multiple control objectives or operates in combination with other controls to achieve a single control objective is necessary for the assurance practitioner in planning the controls testing and in evaluating the findings.

A46. The assurance practitioner may decide to discuss elements of planning with management or other appropriate party when determining the scope of the engagement or to facilitate the conduct and management of the engagement (for example, to co-ordinate some of the planned procedures with the work of the entity's personnel). Although these discussions often occur, the overall engagement strategy and the engagement plan remain the assurance practitioner's responsibility. When discussing matters included in the overall engagement strategy or engagement plan, care is required in order not to compromise the effectiveness of the engagement. For example, discussing the nature and timing of detailed procedures with the entity may compromise the effectiveness of the engagement by making the procedures too predictable.

Materiality (Ref: Para. 34-36, Appendix 1, Appendix 4)

A47. The assurance practitioner applies the same considerations in both limited assurance and reasonable assurance engagements regarding what represents a material control, since such judgements are not affected by the level of assurance being obtained.

A48. The significance to users and the impact on the entity of the achievement of the control objectives provide a frame of reference for the assurance practitioner in considering materiality for the engagement. A materiality matrix may be used to plot the significance to users against the impact on the entity of the control objectives to be concluded upon, as an aid to identifying the material controls. An illustrative example of a materiality matrix is contained in Appendix 4.

A49. In a controls engagement, the decisions of users are influenced by whether and the extent to which the control objectives are achieved, therefore the materiality of a control is dependent on the significance of that control in mitigating the risks which threaten achievement of control objectives. The assurance practitioner obtains an understanding of those risks with respect to the entity as a whole and the activity, function or location relevant to each control objective. Materiality of controls can be assessed in relation to the achievement of overall control objectives or specific control objectives, depending upon which matter the assurance practitioner will conclude on in the assurance practitioner's report.

A50. The assurance practitioner considers the materiality of the controls at the planning stage, reassesses materiality during the engagement based on the findings, and considers the materiality of any identified deficiencies in the design, misstatements in the description, deficiencies in implementation or deviations in the operating effectiveness of those controls.

A51. Materiality of controls is primarily based on qualitative factors, such as:

(a) the significance of the control to achieving a control objective which is to be concluded upon;

(b) whether the control is pervasive in that it impacts on the achievement of multiple control objectives;

(c) the significance to users and impact on the entity or activity of the control objectives which the control seeks to achieve, such as the potential impact on reputation or market confidence which may result from a failure in the operation of the control;

(d) the existence of additional controls which address the same objective, that is the existence of mitigating or compensating controls;

(e) the extent to which the control permeates the business or activities of the entity, such as the impact of a control over a centralised function (for example computer security, central budgeting or human resource management) on other parts of the entity;

(f) users' perceptions and/or interest in the system;

(g) the cost of alternative controls relative to their likely benefit; and

(h) the length of time an identified control was in existence.

A52. Materiality with respect to the operating effectiveness of controls, may also be based on quantitative factors, in particular where the controls relate to activities expressed in volumes or values, such as:

(a) the total value of transactions, volume of relevant activity or quantity of the item or resource to which the control relates;

(b) the number of times the control is applied; or

(c) the economic impact of a control deficiency or deviation, including potential loss of income, increase in expenditure, foregone cost savings or efficiencies, fines or claims against the entity.

Obtaining an Understanding of the Entity's System and Other Engagement Circumstances and Identifying and Assessing Risks of Material Misstatement (Ref: Para. 37-38)

A53. The assurance practitioner's understanding of the system, ordinarily, has a lesser depth for a limited assurance engagement than for a reasonable assurance engagement. The assurance practitioner's procedures to obtain this understanding may include:

- Enquiring of those within the entity who, in the assurance practitioner's judgement, may have relevant information.
- Observing operations.
- Inspecting documents, reports, printed and electronic records.
- Re-performing control procedures.

A54. The nature and extent of procedures to gain this understanding are a matter for the assurance practitioner's professional judgement and will depend on factors such as:

(a) the entity's size and complexity;

(b) the nature of the system to be examined, including the objective(s) to which the control procedures are directed and the risk that those objectives will not be achieved;

(c) the extent to which IT is used; and

(d) the documentation available.

A55. The extent to which an understanding of the IT controls is required, and the level of specialist skills necessary, will be affected by the complexity of the computer system, extent of computer use and importance to the entity, and the extent to which significant control procedures are incorporated into IT systems. The extent of specialist IT skills needed on the assurance team or the need to engage IT experts is identified or clarified during this planning stage.

Identification of Risks (Ref: Para. 37(b)(iii))

A56. As noted in paragraph 17(g), control objectives relate to risks that controls seek to mitigate. The entity is responsible for identifying the risks that threaten achievement of the control objectives which are either stated in the entity's description of its system, Statement of the outcome of the evaluation of controls or agreed with the assurance practitioner in the terms of engagement and identified in the assurance report. The entity 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 designing controls 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 entity's system may itself comprise an informal process for identifying relevant risks.

A57. In practice, in an engagement where there is no description prepared by the responsible party, the assurance practitioner's work in identifying the relevant control objectives to be addressed may help to formalise the risk assessment process.

A58. Consideration of risks may need to go beyond the immediate system. For example, risks may arise as a result of matters which may influence behaviour, such as basis of remuneration, bonuses or the performance measures applied to employees. Factors such as time pressures for completion of processes or activities may result in circumvention of controls.

A59. When identifying and assessing the risk of material control deficiencies or deviations, the assurance practitioner may consider the following factors:

(a) that it is unreasonable for the cost of a control to exceed the expected benefits to be derived;

(b) controls may be directed at routine rather than non-routine transactions or events;

(c) the potential for human error due to carelessness, distraction or fatigue, misunderstanding of instructions and mistakes in judgement;

(d) inconsistency in operation of controls due to automated system interruptions or temporary change in staff due to absences or rotation of roles;

(e) the possibility of circumvention of controls through fraud, which may include the collusion of employees with one another or with parties outside the entity;

(f) the possibility that a person responsible for exercising a control could abuse that responsibility, for example, a member of management overriding a control procedure;

(g) the possibility that management may not be subject to the same controls applicable to other personnel; and

(h) the possibility that controls may become inadequate due to changes in conditions, such as computer systems or operational changes, and compliance with procedures may deteriorate.

Risks Arising from IT

A60. The use of IT affects the way in which control activities are implemented. From the assurance practitioner's perspective, controls over IT systems are effective when they maintain the security, confidentiality, privacy and integrity of the data which such systems process, generate and/or store, through both effective general IT controls and process controls, whilst still providing accessibility and availability of that data so that the operations of the entity are not impeded.

A61. General IT controls are policies and procedures that relate to many software applications and support the effective functioning of process controls. Deficiencies in general IT controls can undermine the effectiveness of process controls and may render those process controls ineffective. General IT controls that maintain the security, confidentiality, privacy, integrity, accessibility and availability of data commonly include controls over the following:

- Data centres, network operations and cloud services.
- Acquisition, development, change management, testing, deployment and maintenance of:
    - Technology infrastructure.
    - Software.
    - Data management systems.
- System access and data transfer security and confidentiality.
- Business continuity, disaster recovery, backup and restoration.

They are generally implemented to deal with the risks referred to in paragraph A64 below.

A62. Process controls are manual or automated procedures that typically operate at a business process level and apply to the processing of data by individual software applications. Process controls can be preventive or detective in nature and are designed to ensure the integrity, including completeness, accuracy, timeliness and authorisation, of the data. Accordingly,

process controls relate to procedures used to initiate, record, process and report data or transactions. These controls help ensure that data or transactions occurred, are authorised, are completely and accurately recorded, processed in the correct period, within an appropriate timeframe and within required service levels. Examples include edit checks of input data, and numerical sequence checks with manual follow-up of exception reports or correction at the point of data entry.

A63. Generally, IT benefits an entity's internal control by enabling an entity to:

(a) consistently apply predefined criteria and perform complex calculations in processing large volumes of transactions or data;

(b) enhance the timeliness, accessibility, availability, and accuracy of information;

(c) facilitate the additional analysis of information;

(d) enhance the ability to monitor the performance of the entity's activities and its policies and procedures;

(e) reduce the opportunity for controls to be circumvented; and

(f) enhance the ability to achieve effective segregation of duties by implementing security controls in software applications, databases, and operating systems.

A64. IT also poses specific risks to an entity's internal control, including, for example:

(a) reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both;

(b) unauthorised access to data that may result in breaches of confidentiality or privacy, deletion or manipulation of data, including the recording of unauthorised or non-existent data, or inaccurate recording of data. Particular risks may arise where multiple users access a common database;

(c) the possibility of personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties;

(d) unauthorised changes to data in master files;

(e) unauthorised changes to systems or programs;

(f) failure to make necessary changes or patches to systems or programs;

(g) inappropriate manual intervention; and

(h) potential loss of data or inability to access data as required.

Risks arising from Manual Controls

A65. Manual elements in internal control may be more suitable where judgement and discretion are required such as for the following circumstances:

- Large, unusual or non-recurring transactions.
- Circumstances where errors are difficult to define, anticipate or predict.
- In changing circumstances that require a control response outside the scope of an existing automated control.
- In monitoring the effectiveness of automated controls.

A66. Manual elements in internal control may be less reliable than automated elements because they can be more easily bypassed, ignored, or overridden and they are also more prone to simple errors and mistakes. Consistency of application of a manual control element cannot therefore be assumed. Manual control elements may be less suitable for the following circumstances:

- High volume or recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented, or detected and corrected, by control parameters that are automated.
- Control activities where the specific ways to perform the control can be adequately designed and automated.

Components of Control (Ref: Para. 38)

A67. The scope of the engagement may require the assurance practitioner to conclude on only certain components of control, such as control activities, within the system and not provide a conclusion on the system as a whole. Nevertheless, the assurance practitioner gains an understanding of the strength of the controls as a whole and in doing so may identify deficiencies in the control environment. A deficiency in the control environment may undermine the effectiveness of controls and this is taken into account in determining the nature, timing and extent of assurance procedures to test the design, implementation and operating effectiveness of controls. For example, the assurance practitioner may consider the "tone at the top" including the entity's track record of adherence to controls, and the monitoring activities, which may include the activities conducted by internal audit. If the control environment or other components of control are assessed as ineffective this will increase the risk of deviations in the operating effectiveness of controls, if included in the scope of the engagement, and impact the nature, timing and extent of assurance procedures.

A68. The assurance practitioner obtains an understanding of the components of control to understand how they may impact the effectiveness of the component which is included in the scope of the engagement. This understanding of the control components may comprise the following:

(a) the control environment, including whether:

  (i) management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behaviour; and

  (ii) the strengths in the control environment elements collectively provide an appropriate foundation for the other components of internal control, and whether those other components are not undermined by deficiencies in the control environment;

(b) risk assessment process, including whether the entity has a process for:

  (i) identifying risks which threaten achievement of control objectives;

  (ii) estimating the significance of the risks;

  (iii) assessing the likelihood of their occurrence; and

  (iv) deciding about actions to address those risks;

(c) the information system and communication including the following areas:

  (i) the entity's operations that are significant to the system;

(ii) the procedures, within both IT and manual systems, by which those functions and services are initiated, recorded, transmitted, processed, corrected as necessary, summarised and reported;

(iii) the records and supporting information that are used to initiate, record, process and report on the system; this includes the correction of incorrect information and how information is summarised. The records may be in either manual or electronic form;

(iv) how the information system captures events and conditions, that are significant to the system; and

(v) the reporting process used to prepare the entity's reports relating to the system, including significant estimates and disclosures;

(d) control activities within the system, being those the assurance practitioner judges are necessary to understand in order to assess the risks of the control objectives not being achieved; and

(e) monitoring activities that the entity uses to monitor controls, including the role of the internal audit function, which mitigate the risks that threaten achievement of the control objectives, and how the entity initiates remedial actions to address deficiencies in design or implementation of controls or deviations in the operating effectiveness of its controls.

A69. The division of internal control into the components, in paragraph A68(a)-(e) above, provides a useful framework for the discussion of different aspects of an entity's internal control which may affect the engagement in this ASAE. However, this does not necessarily reflect how an entity designs, implements and maintains internal control, or how it may classify any particular component. The assurance practitioner may use different terminology or frameworks to describe the various aspects of internal control and their effect on the engagement.

Identifying Risks of Fraud (Ref: Para. 39)

A70. Management is in a unique position to perpetrate fraud because of management's ability to manipulate the entity's records or prepare fraudulent reports by overriding controls that otherwise appear to be operating effectively. Although the level of risk of management override of controls will vary from entity to entity, the risk is nevertheless present in all entities. Due to the unpredictable way in which such override could occur, it is a risk that control objectives will not be achieved due to fraud and thus is a significant risk.

Obtaining an Understanding of the Internal Audit Function (Ref: Para. 40-43)

A71. In obtaining an understanding of the system, including controls, the assurance practitioner determines whether the entity has an internal audit function and its effect on the controls within the system. The internal audit function ordinarily forms part of the entity's internal control and governance structures. The responsibilities of the internal audit function may include, for example, monitoring of internal control, risk management, and review of compliance with laws and regulations, and is considered as part of the assurance practitioner's assessment of risk.

A72. An effective internal audit function may enable the assurance practitioner to modify the nature and/or timing, and/or reduce the extent of assurance procedures performed, but cannot eliminate them entirely.

Obtaining Evidence (Ref: Para. 45-74)

A73. Obtaining evidence on the suitability of the design of controls may be conducted simultaneously with gathering evidence on the description, implementation or operating effectiveness of those controls. The objectives of the engagement are not addressed in isolation so that when gathering evidence on the implementation or operating effectiveness of controls the assurance practitioner may also gain a greater understanding of the design of controls and identify additional or compensating controls relevant to the achievement of the control objectives.

A74. In a direct engagement the assurance practitioner's evaluation of controls and gathering of evidence to support an assurance conclusion on controls, is a single process which results in an assurance conclusion which is also the outcome of the assurance practitioner's evaluation of the controls. Consequently, there is no separate outcome reported by the assurance practitioner in a direct engagement on controls.

A75. An assurance engagement is an iterative process, and information may come to the assurance practitioner's attention that differs significantly from that on which the determination of planned procedures was based. As the assurance practitioner performs planned procedures, the evidence obtained may cause the assurance practitioner to perform additional procedures. In the case of an attestation engagement, such procedures may include asking the responsible party to examine the matter identified by the assurance practitioner, and to make amendments to the description or Statement, if appropriate.

A76. The assurance practitioner may become aware of a matter(s) that causes the assurance practitioner to believe that the controls may not be suitably designed, the description may be materially misstated, the controls may not be implemented as designed or operating effectively. In such cases, the assurance practitioner may investigate such differences by, for example, inquiring of the appropriate party(ies) or performing other procedures as appropriate in the circumstances.

Limited and Reasonable Assurance Engagements (Ref: Para. 46)

A77. The level of assurance obtained in a limited assurance engagement is lower than in a reasonable assurance engagement, therefore the procedures the assurance practitioner performs in a limited assurance engagement are different in nature and timing from, and are less in extent than for, a reasonable assurance engagement. The primary differences between the assurance practitioner's overall responses to assessed risks and further procedures conducted in a reasonable assurance engagement and a limited assurance engagement on controls include:

(a) the emphasis placed on the nature of various procedures as a source of evidence will likely differ, depending on the engagement circumstances. For example, the assurance practitioner may judge it to be appropriate in the circumstances of a particular limited assurance engagement to place relatively greater emphasis on indirect testing of controls, such as enquiries of the entity's personnel, and relatively less emphasis, on direct testing of controls, such as observation, re-performance or inspection, than would may be the case for a reasonable assurance engagement.

(b) in a limited assurance engagement, the further procedures performed are less in extent than in a reasonable assurance engagement in that those procedures may involve:

(i) selecting fewer items for examination;

(ii) performing fewer types of procedures; or

(iii) performing procedures at fewer locations.

Obtaining Evidence Regarding the Design of Controls (Ref: Para. 48-50R)

A78. In evaluating whether a control is suitably designed, either individually or in combination with other controls, to achieve the related control objectives, the assurance practitioner may use flowcharts, questionnaires or decision tables to facilitate understanding the design of the controls.

A79. Controls are directed at preventing, detecting or correcting a failure to achieve a control objective, whether due to fraud or error. Controls may consist of a number of activities directed at the achievement of a control objective. Consequently, if the assurance practitioner evaluates certain activities as being ineffective in achieving a particular control objective, the existence of other activities may allow the assurance practitioner to conclude that controls related to the control objective are suitably designed.

A80. The assurance practitioner's evaluation of the design of the controls includes procedures to assess whether the controls as designed would, individually or in combination with other controls, mitigate the risks which threaten achievement of the identified control objectives, by preventing or detecting and correcting failures to achieve a control objective. These procedures may include:

- Enquiries of management and staff regarding the operation of controls and the types of errors or failures that have occurred or may occur.
- Consideration of flowcharts, questionnaires, decision tables or system descriptions to understand the design.
- Inspection of documents evidencing prevention, detection or correction of failures to achieve a control objective.

A81. When evaluating the suitability of the design of controls to prevent, detect or correct fraud, the assurance practitioner considers whether the following fraud risk factors are adequately mitigated by the designed controls:

(a) any incentives or pressures to commit fraud, such as performance targets, shareholder/investor expectations, results based remuneration or bonuses, reporting or liability thresholds or individual circumstances (such as gambling or personal debts);

(b) perceived opportunities to do so, such as individuals holding a position of trust or inadequate controls; and

(c) any possible rationalisations for doing so, such as underpaid, overworked or otherwise disgruntled employees.

A82. Controls can mitigate but not eliminate the risk of fraud, which may threaten achievement of the identified control objectives. In evaluating the suitability of the design of controls, the assurance practitioner considers whether the controls mitigate the risk of fraud perpetrated by way of:

(a) manipulation, falsification (including forgery) or alteration of records or supporting documentation;

(b) misrepresentation in, or intentional omission from records or reports, relevant events, activities, transactions or other significant information;

(c) intentional misapplication of criteria relating to the measurement or quantification of amounts, classification, manner of presentation or disclosure; or

(d) misappropriation of assets or rights through diversion, stealing, false claims or unauthorised personal use.

A83. Suitably designed controls may be undermined by deficiencies in other components of control or other competing factors within the entity which the assurance practitioner may need to consider. These risks may be addressed through indirect controls, if so these controls may need to be considered in evaluating the suitability of the design of controls.

A84. When evaluating the suitability of the design of controls the assurance practitioner may identify controls which are either included in the design but omitted from the description or included in the description but are ineffective in achieving the control objectives. Where that description is available to users, the assurance practitioner follows the requirements of paragraphs 65 and 66 and clearly identifies the controls to which the conclusion on the design relates.

A85. In a reasonable assurance engagement, when obtaining an understanding of the control environment and considering other components of controls, not included in the scope of the engagement, the assurance practitioner may consider, for example: the tone at the top, extent of management override, the policies regarding recruitment and training of suitably qualified and competent staff and access controls for IT systems. These controls may fall within other components of control not being directly tested, but which may undermine the design, implementation or effective operation of the controls included in the scope of the engagement.

Obtaining Evidence Regarding the Description (Ref: Para.51-52R, Appendix 7)

A86. In obtaining evidence as to whether those aspects of the description included in the scope of the engagement are fairly presented in all material respects, the assurance practitioner determines whether:

- The description addresses the major aspects of the system, being the function or service provided that could reasonably be expected to be relevant to the expected users.
- The description is prepared at a level of detail that provides for the needs of users as reflected in the purpose of the engagement, however, if the description is going to be distributed outside of the entity, it need not be so detailed as to potentially allow a reader to compromise security or other controls at the entity.
- The description accurately reflects the controls as designed and, if included in the scope of the engagement, implemented, which relate to each of the control objectives identified and does not omit or distort information.
- The description identifies any functions or services subject to the engagement which are outsourced to a third party and whether the inclusive or carve-out method has been used with respect to the controls operating at the third party relevant to the control objectives included in the scope of the engagement. If the inclusive method has been used, whether the description clearly distinguishes the controls operating at the entity from the controls operating at the third party.

An example of a description of the system is contained in Appendix 7, example 2.

A87. In obtaining evidence as to whether complementary user-entity or client controls included in the description are adequately described, the assurance practitioner may:

(a) compare the information in the description to contracts with user entities;

(b) compare the information in the description to system or procedure manuals; and

(c) make enquiries of management and staff to gain an understanding of the user entity's responsibilities regarding achieving the control objectives and whether those responsibilities are adequately described.

A88. The assurance practitioner's evaluation of the description may be performed in conjunction with procedures to obtain an understanding of that system. These procedures may include:

- Enquiries of management and staff including, where the scope of the engagement is over a period, specific enquiries about changes in controls that were designed or implemented during the period.
- Observing procedures performed by the entity's personnel.
- Reviewing the entity's policy and procedures manuals and other systems documentation, for example, flowcharts and narratives.
- Reviewing documentary evidence as to the manner in which the controls were implemented.
- Walk-through of control procedures or tracing items through the entity's system.

Obtaining Evidence Regarding Implementation of Controls (Ref: Para. 53-55)

A89. If a control is suitably designed, the assurance practitioner determines, if included in the scope of the engagement, whether the control is implemented by assessing that the implementation process has been carried out so that the control can operate effectively as designed. Implementation is a process, the completion of which can usually be tested on or after the delivery date, although in some cases it may need to be tested during the implementation process if evidence is not available once the control is in place. The nature of the procedures selected by the assurance practitioner to test implementation of controls will depend on the characteristics of the system within which the controls are designed to operate, the processes by which the controls are implemented and the sources of evidence available regarding implementation.

A90. The effective implementation of controls, which enables those controls to operate effectively once they are delivered and in operation, usually involves a number of processes which may include:

- Documentation of controls.
- Development of manuals, instructions and policies for users/operators.
- Allocation of responsibility for operation of each control and procurement or reallocation of human resources to operate and monitor those controls.
- Communication with and training of users/operators in the control methodology and related technology.
- Development or acquisition of IT systems and/or data storage.
- Procurement of outsourced IT services under a service level agreement which specifies controls required to meet the system design.
- Installation, configuration and testing of IT systems and/or data storage.
- Acquisition and installation of equipment, IT hardware, physical security and other infrastructure.
- Establishment of backup for operation of controls in the event of disaster or system failure, such as power outage, infrastructure failure or IT system failure, or routine events, such as staff absences.

Obtaining Evidence Regarding Operating Effectiveness of Controls (Ref: Para. 56-62)

Assessing Operating Effectiveness

A91. If a control is suitably designed the assurance practitioner determines, if included in the scope of the engagement, whether the control is operating effectively by assessing if it operated throughout the period as designed, in all material respects. If suitably designed and operating effectively, a control, individually or in combination with other controls, achieves the related control objectives in all material respects. When the engagement includes operating effectiveness, implementation does not need to be separately tested or concluded upon, as the purpose of effective implementation of a control is that the control will operate effectively.

A92. Evidence about the operation of material controls in prior periods cannot be used as evidence of operating effectiveness of those controls in the current period, however it may be useful in understanding the entity and its environment to identify risks based on past deviations in the operation of controls when planning the engagement. Controls are material to the engagement either when they are themselves to be concluded on in the assurance report or they are material to achieving the control objectives to be concluded on in the assurance report. Controls which are not material to the assurance report conclusion may be tested by rotation for an on-going engagement on controls, in combination with walk-through tests to identify any changes which have occurred to those controls. For example, a three year cycle for the rotation of immaterial controls may be appropriate.

A93. In a limited assurance engagement, ASAE 3000[53] requires the assurance practitioner to identify areas where a material misstatement of the subject matter information is likely to arise. However, in a limited assurance engagement on controls, the assurance practitioner assesses the risks of material deviations in the operating effectiveness of controls, as the requirement in ASAE 3000 cannot be readily interpreted for a controls engagement and may not result in a meaningful conclusion.

A94. The nature of a control procedure often influences the nature of tests of operating effectiveness that can be performed. For example, the assurance practitioner may examine evidence regarding controls where such evidence exists, however documentary evidence regarding some controls often does not exist. In these circumstances, the tests of operating effectiveness may consist of enquiry and observation only. However there is a risk that the control may be triggered by the enquiry and observation and may not operate at other times during the period. Therefore, the assurance practitioner would, in conjunction with those procedures, seek to obtain other supporting evidence by looking to the outcomes from the system, for example substantive testing of the accuracy of the information over which the controls operate.

A95. The decision about what comprises sufficient appropriate evidence is a matter of professional judgement. The assurance practitioner may consider for example:

(a) the nature of the system;

(b) the significance of the control procedure in achieving the relevant objective(s);

(c) the nature and extent of any tests of operating effectiveness performed by the entity in monitoring controls (management, internal audit function or other personnel); and

(d) the likelihood that the control procedure will not reduce to an acceptably low level the risks relevant to the objective(s). This may involve consideration of:

(i) the design effectiveness of the control;

[53] See ASAE 3000, paragraph 46L(a).

(ii) changes in the volume or nature of transactions that might affect design or operating effectiveness (for example, an increase in the volume of transactions may make it tedious to identify and correct errors thereby creating a disincentive to perform the control among entity personnel);

(iii) whether there have been any changes in the control procedure (personnel may not be aware of the change or may not understand the way it operates thus inhibiting effective implementation);

(iv) the interdependence of the control upon other controls (for example the design of controls associated with the cash receipts function may be assessed as effective however their operating effectiveness may be poor due to a lack of segregation of duties);

(v) changes in key personnel who are responsible for performing the control or monitoring its performance (this may result in insufficient knowledge about how the control should operate or lack of awareness of their responsibilities with respect to the control);

(vi) whether the control is manual or automated and the significance of the information system's general controls (manual controls may allow a greater degree of override in a weak control environment, whereas adequately tested IT controls will consistently perform a function based on agreed specifications);

(vii) the complexity of the control (a complex procedure may promote noncompliance if personnel are not adequately trained in the operation of the procedure);

(viii) environmental factors which may influence compliance with the control (employees may circumvent controls when they are time consuming and formal or informal performance assessment relates to speed or throughput);

(ix) whether more than one control achieves the same objective (the assessment of a procedure as ineffective would not necessarily preclude its objective from being achieved as other procedures that are pervasive in nature may address this objective); and

(x) whether there have been any changes in the processes adopted by an entity (for example, a change in a process may render a particular control procedure ineffective).

A96. Obtaining an understanding of controls sufficient to conclude 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. Whether reliance can be placed on the consistent operation of an automated control will depend on the assurance practitioner's assessment and testing of other controls, such as general IT controls, including those over program changes and system access.

A97. To be useful to users and not be potentially misleading, an assurance report on operating effectiveness over a period ordinarily covers a minimum period of six months. The assurance practitioner considers the reasons for a shorter period being selected by the engaging party and whether sufficient instances of the control will be triggered during that period and if there is any indication of bias in the period selected which may avoid possible deviations. If a period

of less than six months is justifiable, the assurance practitioner may consider it appropriate to describe the reasons for the period chosen in the assurance practitioner's assurance report. Circumstances that may result in a report covering a period of less than six months include when:

(a) the assurance practitioner is engaged close to the date by which the report on controls is to be issued;

(b) the system of controls has been in operation for less than six months; or

(c) significant changes have been made to the system of controls and it is not practicable either to wait six months before issuing a report or to issue a report covering the system both before and after the changes.

A98. Certain control procedures may not leave evidence of their operation that can be tested at a later date and, accordingly, the assurance practitioner may find it necessary to test the operating effectiveness of such control procedures at various times throughout the reporting period.

A99. If the assurance practitioner provides a conclusion on the operating effectiveness of controls, that conclusion relates to the operation of controls throughout each period, therefore, sufficient appropriate evidence about the operation of controls during the current period is required for the assurance practitioner to express that conclusion. Knowledge of deviations observed in prior engagements may, however, lead the assurance practitioner to increase the extent of testing during the current period.

A100. Evidence of the operating effectiveness of a control subsequent to period end, for a control which did not operate during the period as it was not triggered, may be used in combination with evidence that the circumstances necessary to trigger the control during the period did not arise and those circumstances were adequately monitored.

Testing of Indirect Controls (Ref: Para. 58L)

A101. In some circumstances, it may be necessary to obtain evidence supporting the effective operation of indirect controls. Controls over the accuracy of the information in exception reports (for example, the general IT controls) are described as "indirect" controls. For example because of the inherent consistency of IT processing, evidence about the implementation of an automated process control, when considered in combination with evidence about the operating effectiveness of the entity's indirect general IT controls (in particular, change controls), may also provide substantial evidence about its operating effectiveness.

Means of Selecting Items for Testing (Ref: Para. 59R)

A102. The means of selecting items for testing available to the assurance practitioner are:

- 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;
- 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
- Sampling: This enables the assurance practitioner to obtain evidence about the items selected in order to form a conclusion about the whole population from which the sample is drawn. Sampling may be appropriate for testing controls that are applied

frequently in a uniform manner and which leave documentary evidence of their application.

A103. 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.

Sampling (Ref: Para. 62)

A104. When designing a controls sample for testing operating effectiveness of controls, the assurance practitioner considers the specific purpose to be achieved and the combination of assurance procedures that is likely to best achieve that purpose, including determining:

- What constitutes a deviation.
- The characteristics of the population to use for sampling and whether that population is complete.
- Whether statistical or non-statistical sampling is to be applied.
- Whether stratification or value-weighted selection is appropriate.
- The sample size based on the level of sampling risk which the assurance practitioner will tolerate.

A105. In considering the characteristics of a population, the assurance practitioner makes an assessment of the expected rate of deviation based on the assurance practitioner's understanding of the relevant controls or on the examination of a small number of items from the population. This assessment is made in order to design a sample and to determine the sample size.

A106. With statistical sampling, sample items are selected in a way that each sampling unit has a known probability of being selected. With non-statistical sampling, judgement is used to select sample items. Because the purpose of sampling is to provide a reasonable basis for the assurance practitioner to draw conclusions about the population from which the sample is selected, it is important that the assurance practitioner selects a representative sample, so that bias is avoided, by choosing sample items which have characteristics typical of the population. The principal methods of selecting samples are the use of random selection, systematic selection and haphazard selection.

A107. Efficiency may be improved if the assurance practitioner stratifies a population by dividing it into discrete sub-populations which have an identifying characteristic. The objective of stratification is to reduce the variability of items within each stratum and therefore allow sample size to be reduced without increasing sampling risk. Controls in a population may be stratified by characteristics, such as the level of approval required, the value or volume of the underlying data, the frequency of the control's application or the complexity of the control's application.[54]

[54] Auditing Standard ASA 530 *Audit Sampling* can be used as further guidance on sampling and sample selection methods.

Evaluating the Evidence Obtained (Ref: Para. 63-74)

Nature and Cause of Deviations (Ref: Para. 68-71)

A108. The deviation rate for the sample of controls tested is also the projected deviation rate for the whole population. The closer the projected deviation rate for a control not operating effectively is to the tolerable rate of deviation, the more likely that actual deviations in the population may exceed tolerable deviations. Also, if the projected deviation rate is greater than the assurance practitioner's expectation of the deviation rate used to determine the sample size, the assurance practitioner may conclude that there is an unacceptable sampling risk that the actual deviations in the population exceed the tolerable deviations. If controls have been divided into strata, the deviation rate applies only to that stratum separately. Projected deviations for each stratum are then combined when considering the possible effect of deviations on the whole population.

A109. Considering the results of other procedures helps the assurance practitioner to assess the risk that actual deviations in the operating effectiveness of controls in the population exceeds tolerable deviations, and the risk may be reduced if additional evidence is obtained. The assurance practitioner might extend the sample size or, unless the controls themselves are being concluded upon (such as when controls are specified by the responsible party or legislation) rather than the control objectives, test alternative or mitigating controls.

- The significance of a deviation or a combination of deviations in the operating effectiveness of a control depends on whether the related control objective was not or is likely to not be achieved as a result and the materiality of the impact of the control objective not being achieved on the assurance practitioner's conclusion.
- Examples of matters that the assurance practitioner may consider in determining whether a deviation or combination of deviations in the operating effectiveness of controls is material include:
    - The likelihood of the deviation/s leading to a material control objective not being achieved.
    - The susceptibility to loss or fraud of the underlying subject matter to which the control applies.
    - The subjectivity and complexity of determining estimated amounts.
    - The monetary value of items exposed to the control deviations.
    - The volume of activity that has been exposed or could be exposed to the control deviations.
    - The importance of the controls to the system and the control objectives; for example:
        - ♦ General monitoring controls (such as oversight of management).
        - ♦ Controls over the prevention and detection of fraud.
        - ♦ Controls over the selection and application of significant accounting or measurement policies.
        - ♦ Controls over significant transactions or activity with related parties.
        - ♦ Controls over significant transactions or activity outside the entity's normal course of business.
        - ♦ Controls over the period-end adjustments.

- The cause and frequency of the exceptions detected as a result of the deviations in the controls.
- The interaction of the deviation with other deviations in internal control.

Indication of Fraud (Ref: Para. 72-73)

A110. In responding to fraud or suspected fraud identified during the engagement, it may be appropriate for the assurance practitioner to, for example:

(a) discuss the matter with the appropriate level of management;

(b) request management to consult with an appropriately qualified third party, such as the entity's legal counsel or a regulator;

(c) consider the implications of the matter in relation to other aspects of the engagement, including the assurance practitioner's risk assessment and the reliability of written representations from the entity;

(d) obtain legal advice about the consequences of different courses of action;

(e) communicate with third parties (for example, a regulator);

(f) withhold the assurance report; or

(g) withdraw from the engagement.

Work Performed by an Assurance Practitioner's Expert (Ref: Para. 75)

A111. ASAE 3000[55] provides application material for the circumstances where an assurance practitioner's expert is involved in the engagement. This material may also be used as helpful guidance when using the work of another assurance practitioner or a responsible party's or evaluator's expert.

Work Performed by Another Assurance Practitioner or a Responsible Party's or Evaluator's Expert (Ref: Para. 76)

A112. The design, description, implementation or operation of an entity's controls may require specialist expertise, such as IT for security and access controls to the IT systems or engineering expertise for calibration of instruments or machinery for measurement of energy usage or production as a basis for controls over completeness of emissions estimations. The necessary experts may be engaged or employed by the entity's management and failure to do so when such expertise is necessary increases the risks of a deficiency in the design, a misstatement in the description, deficiency in the implementation or deviation in operation of the controls.

A113. When information on controls to be used as evidence has been prepared using the work of a responsible party's or evaluator's expert, the nature, timing and extent of procedures with respect to the work of the responsible party's or evaluator's expert may be affected by such matters as:

(a) the nature and complexity of the controls to which the expert's work relates;

(b) the risks of a material deficiency in the design, deficiency in implementation or deviation in operating effectiveness of relevant controls;

[55] See ASAE 3000, paragraphs A120-A134.

(c) the availability of alternative sources of evidence or mitigating controls;

(d) the nature, scope and objectives of the expert's work;

(e) whether the expert is employed by the entity, or is a party engaged by it to provide relevant services;

(f) the extent to which responsible party or evaluator can exercise control or influence over the work of the expert;

(g) whether the expert is subject to technical performance standards or other professional or industry requirements;

(h) the nature and extent of any controls within the entity over the expert's work;

(i) the assurance practitioner's knowledge and experience of the expert's field of expertise; and

(j) the assurance practitioner's previous experience of the work of that expert.

Work Performed by the Internal Audit Function (Ref: Para. 77-79)

A114. The nature, timing and extent of the assurance practitioner's procedures on specific work of the internal auditors will depend on the assurance practitioner's assessment of the significance of that work to the assurance practitioner'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:

(a) examination of evidence of the operation of controls already examined by the internal auditors;

(b) examination of evidence of the operation of other instances of the same controls;

(c) examination of the outcomes of monitoring of controls by internal auditors; and

(d) observation of procedures performed by the internal auditors.

A115. Irrespective of the degree of autonomy and objectivity of the internal audit function, such a function is not independent of the entity as is required of the assurance practitioner when performing the engagement. The assurance practitioner has sole responsibility for the conclusion expressed in the assurance report, and that responsibility is not reduced by the assurance practitioner's use of the work of the internal auditors.

Written Representations (Ref: Para. 80-81)

A116. For application material on using written representations refer to ASAE 3000.[56]

A117. The person(s) from whom the assurance practitioner requests written representations will ordinarily be a member of senior management or those charged with governance. However, because management and governance structures vary by jurisdiction and by entity, reflecting influences such as different cultural and legal backgrounds, and size and ownership characteristics, it is not possible for this ASAE to specify for all engagements the appropriate person(s) from whom to request written representations. The process to identify the appropriate person(s) from whom to request written representations requires the exercise of professional judgement.

[56] See ASAE 3000, paragraphs A136-A139.

A118. Examples of written representations in the form of representation letters are contained in Appendix 6.

Subsequent Events (Ref: Para. 82)

A119. Assurance procedures with respect to the identification of subsequent events after period end are limited to examination of relevant reports, for example reports on control procedures, minutes of relevant committees and enquiry of management or other personnel as to significant non-compliance with control procedures.

A120. The matters identified may provide:

(a) additional evidence or reveal for the first time conditions that existed during the period on which the assurance practitioner is reporting; or

(b) evidence about conditions that existed subsequent to the period on which the assurance practitioner is reporting that may significantly affect the operation of the control procedures.

A121. In the circumstances described in paragraph A120(a), the assurance practitioner reassesses any conclusions previously formed that are likely to be affected by the additional evidence obtained.

A122. In the circumstances described in paragraph A120(b) when the assurance practitioner's report has not already been issued:

(a) in an attestation engagement, the assurance practitioner:

(i) includes an Emphasis of Matter where the responsible party's Statement is available to users and adequately discloses the subsequent event; or

(ii) issues a qualified conclusion if the responsible party's Statement is available to users and does not adequately disclose the subsequent event; and

(b) in a direct engagement, the assurance practitioner includes a paragraph in the assurance report headed "Subsequent Events" describing the events and indicating that the subsequent events do not impact the assurance conclusion but they may affect the future effectiveness of the control procedures.

A123. The assurance practitioner does not have any responsibility to perform procedures or make any enquiry after the date of the report. If however, after the date of the report, the assurance practitioner becomes aware of a matter identified in paragraph A120, the assurance practitioner considers re-issuing the report. In an attestation engagement where the report has already been issued, the new report includes an Emphasis of Matter discussing the reason for the new report. In a direct engagement, the new report discusses the reason for the new report under a heading "Subsequent Events".

Other Information (Ref: Para. 83)

A124. Relevant ethical requirements require that an assurance practitioner not be associated with information where the assurance practitioner 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.[57]

A125. If other information included in a document containing the assurance practitioner's report includes future-oriented information such as recovery or contingency plans, or plans for modifications to the system that will address deficiencies or deviations identified in the assurance practitioner's report, or claims of a promotional nature that cannot be reasonably substantiated, the assurance practitioner may request that information be removed or restated.

A126. Scrutiny of documents containing the assurance practitioner's report which is to be made publicly available is more critical than reports to be distributed internally within the responsible party or amongst other users who are knowledgeable about the circumstances of the engagement.

Forming the Assurance Conclusion (Ref: Para. 84-87)

A127. Control consists of a number of integrated processes directed at the achievement of specific control objectives, which together contribute to the achievement of overall objectives. The scope of the assurance practitioner's engagement may be centred on the achievement of overall objectives or may go to the level of specific objectives. Some controls may have a pervasive effect on achieving many overall objectives, whereas others are designed to achieve a specific objective. Because of the pervasive nature of some controls, the assurance practitioner may find several controls that affect the risks relevant to a particular objective. Consequently, when the assurance practitioner evaluates a control as being unsuitably designed, not implemented as designed or operating ineffectively to achieve a specific objective the assurance practitioner does not, on this basis alone, conclude that that objective will not be achieved. The assurance practitioner will also need to consider the effect of this evaluation on the operation of other related controls and identify any compensating controls which may mitigate the ineffective control, in order to determine the effect of the ineffective control on the assurance practitioner's conclusion.

A128. In assessing the impact of uncorrected deficiencies in the design, misstatements in the description, deficiencies in the implementation or deviations in operating effectiveness of controls, the assurance practitioner considers the impact of those matters on each other. For example, controls may still be suitably designed, implemented as designed and operating effectively, even if the description is materially misstated and does not appropriately reflect the controls as designed. However, if the design of controls is unsuitable, the assurance practitioner does not test the implementation or operating effectiveness of those unsuitable controls and the assurance practitioner's conclusion on implementation or operating effectiveness relates only to the controls which are suitably designed.

Preparing the Assurance Report

Assurance Report Content (Ref: Para. 88-91, Appendix 8, Appendix 9)

A129. A statement of the limitations of controls in the assurance report states that:

(a) because of inherent limitations in any system, it is possible that fraud, error, or non-compliance with laws and regulations may occur and not be detected. Further, the system, within which the control procedures that have been assured operate, has not been assured and no conclusion is provided as to its effectiveness;

(b) a reasonable/limited assurance engagement, which includes operating effectiveness of controls, is not designed to detect all instances of controls operating ineffectively as it

[57] See ASA 102.

is not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis; and

(c) any projection of the outcome of the evaluation of the controls to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

A130. The assurance practitioner may expand the report to include other information not intended as a qualification of the assurance practitioner's conclusion. If the report includes other information it is a long-form report as the information is additional to the basic elements required in paragraph 89 for a short-form report. This additional information may be required by regulation or agreed in the terms of engagement to meet the needs of users. When considering whether to include any such information the assurance practitioner assesses the materiality of that information in the context of the objectives of the engagement. Other information is not to be worded in such a manner that it may be regarded as a qualification of the assurance practitioner's conclusion and may include for example:

- A description of the facts and findings relating to particular aspects of the engagement.
- The specific control objectives, related controls, the tests of controls that were performed and the results of those tests.
- Recommendations for improvements to address identified control design deficiencies, implementation deficiencies or deviations in operating effectiveness.
- Control deficiencies or deviations not considered significant because the cost of the control exceeds the benefit.

A131. If the terms of the engagement require the results of the tests of controls to be reported, then the assurance practitioner, in describing the tests of controls, clearly states which controls were tested, identifies whether the items tested represent all or a selection of the items in the population, and indicates the nature of the tests in sufficient detail to be useful to users. If deviations have been identified, the assurance practitioner includes 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 assurance practitioner reports deviations even if, on the basis of tests performed, the assurance practitioner has concluded that the related control objective was achieved.

A132. If the criteria are adequately described in a source that is readily accessible to the intended users of the assurance practitioner's report, the assurance practitioner may identify those criteria by reference, rather than by repetition in the assurance practitioner's report or an appendix to the report, for example, if the criteria are published and generally available, or if they are detailed in a description of the system. The controls designed to achieve the controls objectives, as criteria for implementation or operating effectiveness of controls, are not usually detailed in the assurance report, unless set out in the description of the system. As the control objectives provide the criteria for evaluation of the design of controls, against which implementation or operating effectiveness are then evaluated, the control objectives also provide the criteria for the controls engagement as a whole. Consequently, in making the criteria available to users it is usually sufficient for the control objectives to be identified.

Specific Purpose (Ref: Para. 89(g))

A133. In some cases the control objectives used to assess the controls may be identified for a specific purpose. For example, a regulator may require certain entities to use particular criteria designed for regulatory purposes. To avoid misunderstandings, the assurance practitioner alerts users of the assurance report to this fact and that, therefore, the description of controls may not be suitable for another purpose.

A134. The assurance practitioner may consider it appropriate to indicate that the assurance report is intended solely for specific users. Depending on the engagement circumstances, for example, the law or regulation of the particular jurisdiction, this may be achieved by restricting the distribution or use of the assurance report. While an assurance report may be restricted in this way, the absence of a restriction regarding a particular user or purpose does not itself indicate that a legal responsibility is owed by the assurance practitioner in relation to that user or for that purpose. Whether a legal responsibility is owed will depend on the legal circumstances of each case and the relevant jurisdiction.

Summary of the Work Performed (Ref: Para. 89(m))

A135. The summary of the work performed helps the intended users understand the nature of the assurance conveyed by the assurance report. For many assurance engagements, infinite variations in procedures are possible in theory. It may be appropriate to include in the summary a statement that the work performed included evaluating the suitability of the control objectives and the risks that threaten achievement of those objectives.

A136. In a limited assurance engagement an appreciation of the nature, timing, and extent of procedures performed is essential to understanding the assurance conveyed by the conclusion, therefore the summary of the work performed is ordinarily more detailed than for a reasonable assurance engagement and identifies the limitations on the nature, timing, and extent of procedures. It also may be appropriate to indicate certain procedures that were not performed that would ordinarily be performed in a reasonable assurance engagement. However, a complete identification of all such procedures may not be possible because the assurance practitioner's required understanding and consideration of engagement risk is less than in a reasonable assurance engagement.

A137. Factors to consider in determining the level of detail to be provided in the summary of the work performed include:

(a) circumstances specific to the entity (e.g. the differing nature of the entity's control environment compared to those typical in the sector);

(b) specific engagement circumstances affecting the nature and extent of the procedures performed; and

(c) the intended users' expectations of the level of detail to be provided in the report, based on market practice, or applicable law or regulation.

A138. It is important that the summary be written in an objective way that allows intended users to understand the work done as the basis for the assurance practitioner's conclusion. In most cases this will not involve relating the entire work plan, but on the other hand it is important for it not to be so summarised as to be ambiguous, nor written in a way that is overstated or embellished.

A139. Illustrative examples of assurance practitioner's reports are contained in Appendix 8.

Intended Users and Purposes of the Assurance Report (Ref: Para. 89(g))

A140. If the assurance practitioner's report on controls has been prepared for a specific purpose and is only relevant to the intended users, this is stated in the assurance practitioner's report. In addition, the assurance practitioner 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.

Modified Conclusions (Ref: Para. 93-95)

A141. Modifications to the assurance report may be made in the following circumstances:

(a) a qualified conclusion may be issued if the following matters are material but not pervasive:

(i) unsuitable criteria mandated by legislation or regulation;

(ii) scope limitation;

(iii) deficiency in the design of controls to achieve each material control objective;

(iv) misstatement in the description;

(v) deficiency in the implementation of controls as designed; or

(vi) deviation in the operating effectiveness of controls.

(b) an adverse conclusion may be issued if the following matters are both material and pervasive:

(i) unsuitable criteria mandated by legislation or regulation;

(ii) deficiency in the design of controls to achieve the control objectives;

(iii) misstatement in the description;

(iv) deficiency in the implementation of controls as designed; or

(v) deviation in the operating effectiveness of controls.

(c) a disclaimer may be issued if there is a limitation of scope which is both material and pervasive.

A142. Examples of matters which the assurance practitioner may assess as both material and pervasive and warrant an adverse conclusion include:

(a) deficiencies in the design of controls which result in the controls being unsuitable to achieve a significant proportion of the control objectives in the scope of the engagement, for which no, or insufficient, suitably designed compensating controls exist;

(b) deficiencies in the implementation of controls so that they will not be able to operate as designed which may or will result in a significant proportion of the control objectives in the scope of the engagement not being achieved when the controls are in operation; or

(c) deviations in the operating effectiveness of controls which may or do result in a significant proportion of the control objectives in the scope of the engagement not being achieved, for which no, or insufficient, suitably designed compensating controls exist.

A143. Typically, misstatements in the description, however extensive, alone do not result in an adverse conclusion. If controls have been designed suitably to achieve the control objectives, but those controls are not presented fairly or are misstated in the description, if the entity is able to change that description it would be appropriate to do so. If the entity declines or is unable to amend the description, the assurance conclusion is qualified with respect to the description, however the controls which would achieve the control objectives can be identified in the assurance report and their design, implementation or operating effectiveness are able to be assured.

A144. Each control objective is considered individually and in combination with other objectives to assess the impact on the assurance report. Deficiencies in the design, implementation or

operating effectiveness of controls to achieve an individual control objective may result in a qualification if that control objective is material to the system that is subject to the engagement.

A145. Whenever the assurance practitioner expresses a qualified conclusion, the assurance practitioner's report includes a clear description of all the substantive reasons therefor, and:

(a) a description of the effect of all identified matters on the residual risk of not achieving relevant control objectives; or

(b) if the assurance practitioner is unable to reliably determine the effect of a matter, a statement to that effect.

A146. Illustrative examples of elements of modified assurance practitioner's reports are contained in Appendix 9.

A147. Even if the assurance practitioner has expressed an adverse conclusion or a disclaimer of conclusion, it may be appropriate to describe in the basis for modification paragraph the reasons for any other matters of which the assurance practitioner is aware that would have required a modification to the conclusion, and the effects thereof.

A148. When expressing a disclaimer of conclusion, because of a scope limitation, it is not ordinarily appropriate to identify the procedures that were performed nor include statements describing the characteristics of the assurance practitioner's engagement; to do so might overshadow the disclaimer of conclusion.

Other Communication Responsibilities (Ref: Para. 96-98)

A149. Appropriate actions to respond to the circumstances identified in paragraph 96 may include:

- Obtaining legal advice about the consequences of different courses of action.
- Communicating with those charged with governance of the entity.
- Communicating with third parties (for example, a regulator) when required to do so.
- Modifying the assurance practitioner's conclusion, or adding an Other Matter paragraph.
- Withdrawing from the engagement.

A150. Certain matters identified during the course of the engagement may be of such importance that they would be communicated to those charged with governance. Unless stated otherwise in the terms of engagement, less important matters would be reported to a level of management that has the authority to take appropriate action.

Documentation (Ref: Para. 99-100)

A151. For application material on preparing and maintaining documentation refer to ASAE 3000.[58]

*** * ***

[58] See ASAE 3000, paragraphs A200-A207.

Appendix 1

(Ref: Para. A15, A16, A29-A34, A49)

NATURE OF ASSURANCE ENGAGEMENTS ON CONTROLS

Scope of the Engagement

A summary of the scope of assurance engagements which may be conducted with respect to controls is set out in the following table:

Scope of Engagement	Subject Matter	Criteria for Evaluating Subject Matter	Outcome of the Evaluation (Subject Matter Information)	Basis of Materiality	Date or Period Covered
Suitability of design of controls to achieve identified control objectives	Controls as designed	Control objective/s.	Evaluator's Statement or assurance practitioner's conclusion whether controls are suitably designed to achieve the control objectives.	Significance of control in mitigating the risks which threaten achievement of each control objective.	As at date or throughout the period.[59]
And, if included in the scope of the engagement:					
Fair presentation of description of the system; and/or	Description of the system	Completeness and accuracy of controls as designed.	Evaluator's Statement or assurance practitioner's conclusion whether the description is fairly presented.	Significance of control in mitigating the risks which threaten achievement of each control objective and significance of matters described to understanding system of controls.	As at date or, throughout the period.[59]
Implementation of controls as designed; or	Controls implemented	Controls as designed, necessary to achieve the control objectives.	Evaluator's Statement or assurance practitioner's conclusion whether the controls were implemented as designed.	Significance of control in mitigating the risks which threaten achievement of each control objective.	As at date.
Operating effectiveness of controls as designed	Controls in operation	Controls as designed, necessary to achieve the control objectives.	Evaluator's Statement or assurance practitioner's conclusion whether the controls operated effectively as designed.	Significance of control in mitigating the risks which threaten achievement of each control objective.	Throughout the period.

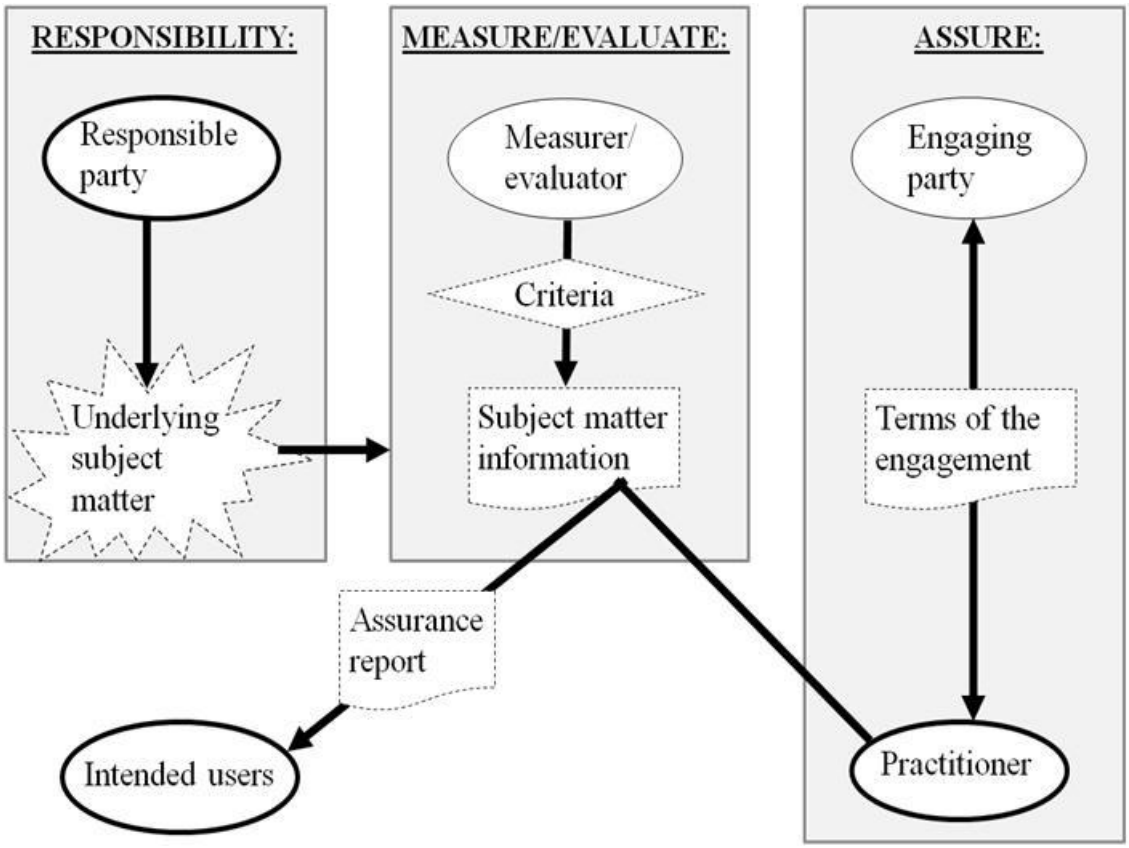
[59] The engagement can only cover "throughout the period" if operating effectiveness is included in the scope of the engagement.

Appendix 2

(Ref: Para. A7, A15, A16)

ROLES AND RESPONSIBILITIES

Diagram from Appendix 1 of ASAE 3000 Explained in the Context of Assurance Engagements on Control.



Notes on the Application of the Terms and Roles in the Above Diagram to Assurance Engagements on Controls Conducted under this ASAE.

1. The equivalent terms in an assurance engagement on controls to those in the above diagram are:

   (a) Criteria - the control objectives for evaluating the design of controls and the design of controls for evaluating the description, implementation and operating effectiveness of controls. This ASAE also provides additional criteria to consider.

   (b) Subject matter information – the responsible party or evaluator's Statement in an attestation engagement and the assurance practitioner's report in a direct engagement.

   (c) Underlying subject matter – the controls within the system designed to achieve the control objectives and, if included in the scope of the engagement, the description of the system, the controls implemented or the controls in operation.

The other terms used in the diagram above also apply to assurance engagements on controls.

2. The roles illustrated in the above diagram relate to an assurance engagement on controls as follows:

   (a) The responsible party is responsible for the design of controls and, if included in the scope of the engagement, the description of the system and/or implementation or operation of controls.

   (b) The measurer/evaluator (evaluator in this standard) uses the control objectives to evaluate the design of the controls and, if included in the scope of the engagement, uses the controls as designed to evaluate the description of the system, implementation or operating effectiveness of controls. This evaluation results in a Statement in an attestation engagement or the assurance practitioner's conclusion in a direct engagement.

   (c) The engaging party agrees the terms of the engagement with the assurance practitioner.

   (d) The practitioner (assurance practitioner in this standard) obtains sufficient appropriate evidence in order to express a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the design, description, implementation and/or operating effectiveness of controls.

   (e) The intended users make decisions on the basis of the responsible party or evaluator's Statement or the assurance practitioner's conclusion. The intended users are the individual(s) or organisation(s), or group(s) thereof that the assurance practitioner expects will use the assurance report.

Appendix 3

(Ref: Para. 14)

STANDARDS APPLICABLE TO ENGAGEMENTS ON CONTROLS

		APPLICABLE AUASB STANDARDS				
		ASAE 3000 Assurance Engagements (not Historical Financial Info)	**ASAE 3150 Assurance Engagements on Controls (This ASAE)**	**ASAE 3402 Controls at a Service Organisation**	**ASAE 3100 Compliance Engagements**	**ASRS 4400 Agreed-upon Procedures Engagements**
Subject Matter of Controls Assurance Engagement	1. Entity's controls over:					
	- Financial reporting	✓	✓			
	- Non-financial reporting	✓	✓			
	- Services or functions	✓	✓			
	2. Entity's controls over compliance with requirements[60]	✓	✓			
	3. Entity's compliance with requirements specifying controls	✓			✓[61]	
	4. Service Organisation's controls:					
	- Relevant to user entities' non-financial reporting, services or functions	✓	✓			
	- Relevant to user entities' financial reporting	✓		✓		
	5. Controls over economy, efficiency or effectiveness	✓	✓			
	6. Procedures restricted to those specified by engaging party					✓

[60] Where controls not specified in law, regulation or quasi-regulation.
[61] This ASAE may provide useful guidance for engagements on entity's compliance with requirements specifying controls.

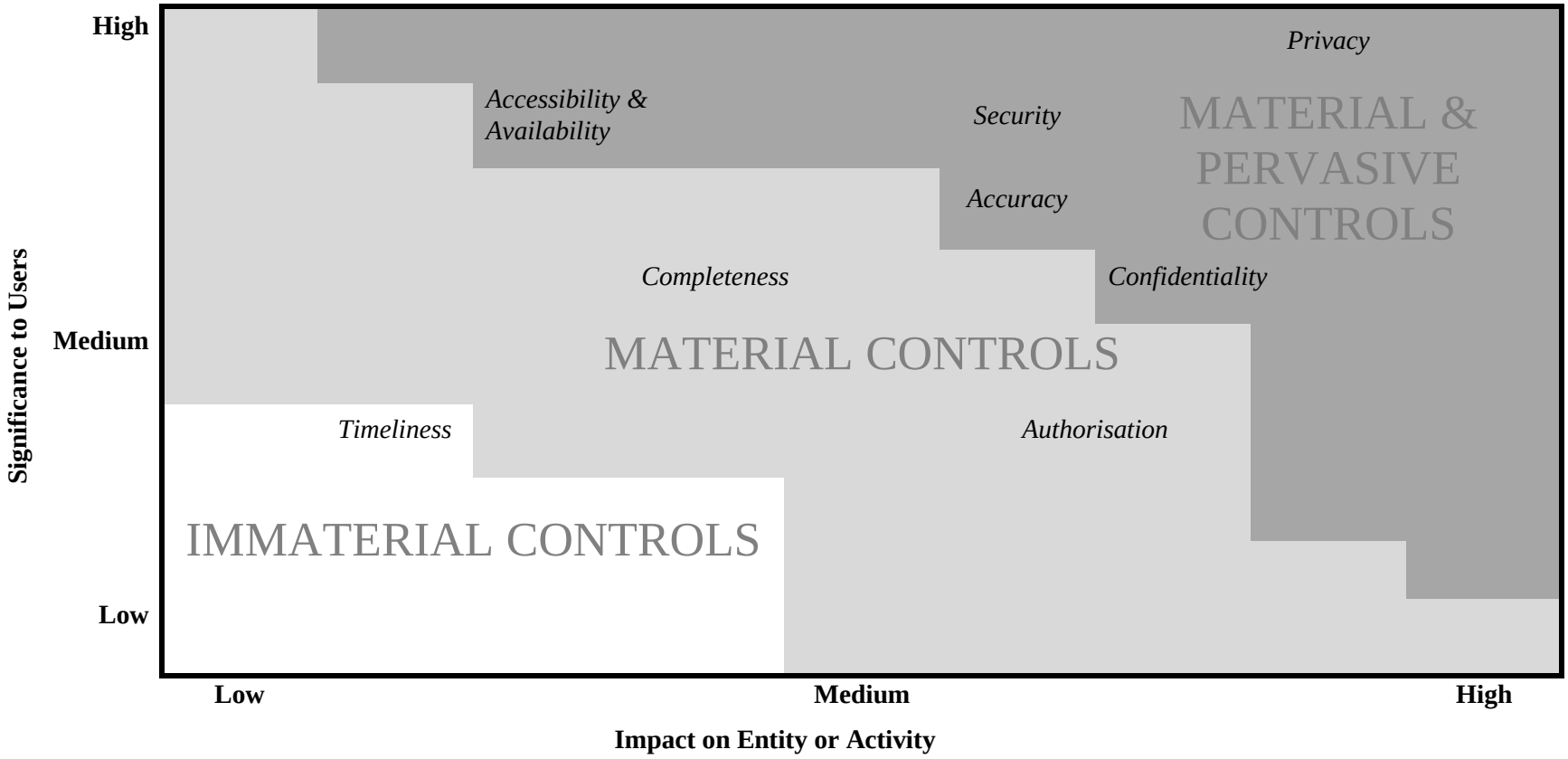
Appendix 4

(Ref: Para. A48)

EXAMPLE MATERIALITY MATRIX FOR OVERALL CONTROL OBJECTIVES

Assurance Engagement on Controls over Services for Processing Client's Employee Data

This matrix depicts an example of overall control objectives (see paragraph A19(e)) and illustrates the evaluation of the materiality of controls related to those objectives relevant to the contractual obligations of a service organisation processing client's employee data.



Appendix 5

(Ref: Para. A36)

EXAMPLE ENGAGEMENT LETTERS

Example 1: Engagement Letter for an Attestation Engagement for Limited Assurance on the Design and Description of Controls

Example 2: Engagement Letter for an Attestation Engagement for Reasonable Assurance on the Design, Description and Operating Effectiveness of Controls

Example 3: Engagement Letter for a Direct Engagement for Reasonable Assurance on the Design and Implementation of Controls

The following examples of assurance practitioner's engagement letters are for guidance only and are not intended to be exhaustive or applicable to all situations.

Example 1: Engagement Letter for an Attestation Engagement for Limited Assurance on the Design and Description of Controls

To [*the appropriate representative of management or those charged with governance of ABC or the engaging party*]:

[*The objective and scope of the engagement*]

You have requested that we undertake a limited assurance engagement on ABC's Statement [which will accompany our report] regarding the design of controls over [*specify function/location/boundaries of the controls*][62] and the description of ABC's [*the type or name of*] system, which you will provide and which will accompany our report, as at [*date*] for the purpose of reporting to [*identify intended users: the Board of Directors/Regulator/Customers of ABC*]. The description of ABC's [*the type or name of*] system comprises control objectives and related controls designed to achieve those objectives. The control objectives to be addressed [were identified or developed by ABC/are specified by legislation/regulation], which are: [*list objectives/requirements or identify them by reference*].

We are pleased to confirm our acceptance and our understanding of this limited assurance engagement by means of this letter. Our assurance engagement will be conducted with the objective of reaching a conclusion on [ABC's Statement regarding][63] the suitability of the design of the controls within ABC's [*the type or name of*] system to achieve the stated control objectives and the fair presentation of the description of [t*he type or name of*] system as at [*date*].

[*Responsibilities of the assurance practitioner*]

We will conduct our assurance engagement in accordance with Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls*. That standard requires that we comply with ethical requirements applicable to assurance engagements and plan and perform procedures to obtain limited assurance about whether anything has come to our attention that causes us to believe that [ABC's Statement is not fairly presented in that] the controls within ABC's [*the type or name of*] system are not suitably designed to achieve the control objectives or the description of the system is not fairly presented, in all material respects. An assurance engagement involves performing procedures to obtain evidence about the design of controls and description of the system. The procedures selected depend on the assurance practitioner's professional judgement, including the assessment of the risks of material deficiencies in the design of the controls or misstatements in the description of the [*type or name of*] system. We will perform procedures primarily consisting of making enquiries of

[62] If a specific control component is being reported on only, specify that control component, which will depend on the control framework applied and are most commonly control activities, but may also include: the control environment, risk assessment, information and communication or monitoring activities.

[63] Insert if the assurance report is expressed in terms of the responsible party's or evaluator's Statement rather than the underlying subject matter.

management and others within the entity, as appropriate, examination of design specification and documentation and evaluation of the evidence obtained about the design of controls and description of the system. We will also perform additional procedures if we become aware of matters that cause us to believe the controls may not be suitably designed or the description may not be fairly presented. The procedures selected depend on what we consider necessary applying our professional judgement, including the assessment of the risks of material deficiencies in the design or misstatements in the description of the [*type or name of*] system.

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

The system, within which the controls that we will test operate, will not be examined except to the extent the system is relevant to the achievement of the control objectives. Therefore no opinion will be expressed as to the effectiveness of the system of controls as a whole.

The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement and consequently the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed. Therefore there is a higher risk than there would be in a reasonable assurance engagement, that any material deficiencies in the design of controls that exist may not be revealed by the engagement, even though the engagement is properly performed in accordance with ASAE 3150. In expressing our conclusion, our report on the design of controls and description of the system will expressly disclaim any reasonable assurance conclusion on controls.

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

Our assurance engagement will be conducted on the basis that [the responsible party/ management/ those charged with governance] acknowledges and understands that they have responsibility:

(a) for the preparation of a written Statement [which will be attached to our report] that throughout the period, in all material respects, and based on suitable criteria:

  (i) the controls within ABC's [*the type or name of*] system were suitably designed to achieve the identified control objectives; and

  (ii) the description fairly presents ABC's [*the type or name of*] system as designed, including changes in controls;

(b) for the identification of suitable control objectives which [are specified by [law/ regulation/ contract/ another party]/ developed by the responsible party or assurance practitioner] to address [*specify overall objectives*] in relation to the system;

(c) for the identification of risks that threaten achievement of the control objectives identified above;

(d) for design of the system, comprising controls which will mitigate those risks, so that those risks will not prevent achievement of the identified control objectives, and therefore the control objectives will be achieved;

(e) for preparation of a description of the system, including identification of any controls operated by a third party, service or sub-service organisation and whether the inclusive or carve-out method has been used in relation to those third party controls; and

(f) 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 and description of the controls within ABC's [*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.

(g) [if controls designed to be operated by a third party, service or sub-service organisation, may be material to the engagement, to obtain either:

(i) a limited assurance report on the design and description of controls which covers the relevant controls at the third party; or

(ii) access to all information relevant to the design and description of those controls, any additional information requested and access to persons from whom to obtain evidence at the third party.][64]

As part of our engagement, we will request from [the responsible party/ management/ those charged with governance] written confirmation concerning representations made to us in connection with the engagement [and written confirmation concerning any representations made by the third party, where material controls designed at that third party are included in the scope of the engagement].[64]

[*Assurance Approach*]

We will develop/identify the control objectives and related controls for [*the type or name of*] system described above.

Our procedures will extend to the control objectives and related controls at relevant third parties only to the extent that those controls are included in ABC's description of [*the type or name of*] system and are necessary to achieve the relevant control objectives.

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

[*Assurance Procedures*]

Our assurance procedures will include:

(a) obtaining an understanding of the control environment of ABC relevant to the [*type or name of*] system;

(b) developing or identifying suitable control objectives;

(c) evaluating the design of specific controls by:

(i) assessing the risks that threaten achievement of the control objectives; and

(ii) evaluating whether the controls as designed are capable of addressing those risks and achieving the related control objectives; and

(d) evaluating the completeness, accuracy and presentation of the Description of the [*type or name of*] System against the controls as designed.

[64] Insert if controls which may be material to the engagement are operated by a third party, service or sub-service organisation.

[In undertaking this engagement, we will work closely with ABC's internal audit function and we intend to place reliance on its work in accordance with ASAE 3000 *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information.*][65]

[*Assurance Report*]

The format of the report will be in accordance with ASAE 3150 with respect to limited assurance engagements [and will be in long-form, including controls designed to achieve each control objective, assurance procedures and findings]. An example of the proposed report is contained in the appendix to this letter.

[*Use of the Assurance Report*][66]

[Our report is prepared for the use of ABC and [*intended users*] for [*purpose*] and may not be suitable for any other purpose.

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 ABC and [*intended users*], or for any purpose other than that for which it was prepared.]

[*Material Deficiencies in Design of Controls or Misstatements in the Description of the System*]

We will issue an assurance report without modification, to provide a limited assurance conclusion on the controls within the [*type or name of*] system where our procedures do not bring a material deficiency in the design of controls necessary to achieve the control objectives identified or a material misstatement in the description of the system to our attention. For this purpose, a material deficiency exists when:

(a) the controls as designed will not or may not achieve the control objectives in all material respects or the description contains material inaccuracies, inadequacies or omissions; and

(b) knowledge of that deficiency or misstatement would be material to users of the assurance report.

If our assurance engagement identifies that there are material deficiencies in the design of controls during the period covered by the report, such deficiencies will be disclosed in our report. If any material deficiencies disclosed in our report have been corrected subsequent to [*date*] (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 may also provide you with a letter containing recommendations for strengthening controls if such matters are observed during the process of the assurance engagement. Although issues raised may not represent deficiencies in design of the controls or misstatements in the description of the system which are material to our conclusion, our 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 controls within the [*the type or name of*] system, including our respective responsibilities.

---

[65] Insert this sentence if the work of internal audit is an integral part of the assurance engagement.
[66] Insert this section if the report is to be for restricted use only.

Yours faithfully,

(signed)

……

Name and Title

Date

Acknowledged on behalf of [*engaging party*]

(signed)

…….

Name and Title

Date

Example 2: Engagement Letter for an Attestation Engagement for Reasonable Assurance on the Design, Description and Operating Effectiveness of Controls

To [*the appropriate representative of management or those charged with governance of ABC or the engaging party*]:

[*The objective and scope of the engagement*]

You have requested that we undertake a reasonable assurance engagement on ABC's Statement [which will accompany our report] regarding the design of controls over [*specify function/location/boundaries of the controls*],[67] the description of ABC's [*the type or name of*] system, which you will provide and which will accompany our report, and the operating effectiveness of controls throughout the period [*date*] to [*date*] (the period) for the purpose of reporting to [*identify intended users: the Board of Directors/Regulator/Customers of ABC*]. The description of ABC's [*the type or name of*] system comprises control objectives and related controls designed to achieve those objectives for the [*period*] ended [*date*]. The control objectives to be addressed [were identified or developed by ABC/are specified by legislation/regulation], which are: [*list objectives/requirements or identify them by reference*].

We are pleased to confirm our acceptance and our understanding of this reasonable assurance engagement by means of this letter. Our assurance engagement will be conducted with the objective of expressing an opinion on [ABC's Statement regarding][68] the suitability of the design of controls within ABC's [*the type or name of*] system to achieve the stated control objectives, the fair presentation of the description of [*the type or name of*] system and the operating effectiveness of those controls throughout the period.

[*Responsibilities of the assurance practitioner*]

We will conduct our assurance engagement in accordance with Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls*. That standard requires that we comply with ethical requirements applicable to assurance engagements and plan and perform procedures to obtain reasonable assurance about whether, in all material respects, [ABC's Statement that] the controls are suitably designed to achieve the control objectives, the description of the [*type or name of*] system is fairly presented and the controls operated effectively throughout the period [is fairly stated]. An assurance engagement involves performing procedures to obtain evidence about the design, description and operating effectiveness of controls. The procedures selected depend on the assurance practitioner's professional judgement, including the assessment of the risks of material deficiencies in the design, misstatements in the description or deviations in the operating effectiveness of controls within the [*type or name of*] system.

Because of the inherent limitations of an assurance engagement, together with the inherent limitations of any system of controls there is an unavoidable risk that some deficiencies in the design, misstatements in the description or deviations in the operating effectiveness of controls may not be detected, even though the engagement is properly planned and performed in accordance with Standards on Assurance Engagements.

The system, within which the controls that we will test operate, will not be examined except to the extent the system is relevant to the achievement of the control objectives. Accordingly, no opinion will be expressed as to the effectiveness of the system of controls as a whole.

---

[67] If a specific control component is being reported on only, specify that control component, which will depend on the control framework applied and are most commonly control activities, but may also include: the control environment, risk assessment, information and communication or monitoring activities.

[68] Insert if the assurance report is expressed in terms of the responsible party's or evaluator's Statement rather than the underlying subject matter.

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

Our assurance engagement will be conducted on the basis that [the responsible party/management/those charged with governance] acknowledges and understands that they have responsibility:

(a) for the preparation of a written Statement [which will be attached to our report] that throughout the period, in all material respects, and based on suitable criteria:

  (i) the controls within ABC's [*the type or name of*] system were suitably designed to achieve the identified control objectives; and

  (ii) the description fairly presents ABC's [*the type or name of*] system as designed, including changes in controls; and

  (iii) the controls stated in ABC's description of its system operated effectively to achieve the control objectives;

(b) for the identification of suitable control objectives which [are specified by [law/ regulation/ contract/ another party]/ developed by the responsible party or assurance practitioner to address [*specify overall objectives*] in relation to the system];

(c) for the identification of risks that threaten achievement of the control objectives identified;

(d) for design of the system, comprising controls which will mitigate those risks so that those risks will not prevent achievement of the identified control objectives and therefore that the control objectives will be achieved;

(e) for preparation of a description of the system, including identification of any controls operated by a third party, service or sub-service organisation and whether the inclusive or carve-out method has been used in relation to those third party controls;

(f) for operation of the controls as designed throughout the period;

(g) to provide us with:

  (i) access to all information of which those charged with governance and management are aware that is relevant to the description of the [*the type or name of*] system and design and operation of the controls within that 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.

(h) [if controls designed to be operated by a third party, service or sub-service organisation, are included in the description of the system (the inclusive method) and may be material to the engagement, to obtain either:

  (i) a reasonable assurance report on the design, description and operating effectiveness of controls which covers the relevant controls at the third party; or

  (ii) access to all information relevant to the design, description and operation of those controls, any additional information requested and access to persons from whom to obtain evidence at the third party.][69]

[69] Insert if controls which may be material to the engagement are operated by a third party, service or sub-service organisation.

As part of our engagement, we will request from [the responsible party/ management/ those charged with governance] written confirmation concerning representations made to us in connection with the engagement [and written confirmation concerning any representations made by the third party, where material controls operated at that third party are included in the description].[70]

[*Assurance Approach*]

We will examine and evaluate the control objectives and controls for [*the type or name of*] system described above.

Our procedures will extend to the control objectives and related controls at relevant third parties only to the extent that those controls are included in ABC's description of [*the type or name of*] system and are necessary to achieve the relevant control objectives.

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

[*Assurance Procedures*]

Our assurance procedures will include:

(a) obtaining an understanding of the control environment of ABC relevant to the [*type or name of*] system;

(b) evaluating the suitability of the control objectives;

(c) evaluating the design of specific controls by:

  (i) assessing the risks that threaten achievement of the control objectives; and

  (ii) evaluating whether the controls described are capable of addressing those risks and achieving the related control objectives;

(d) evaluating the completeness, accuracy and presentation of the Description of the [*type or name of*] System against the controls as designed; and

(e) making enquiries, inspecting documents, conducting walk throughs and re-performance of controls to ascertain whether the degree of compliance with controls is sufficient to achieve their control objectives throughout the period.

[In undertaking this engagement, we will work closely with ABC's internal audit function and we intend to place reliance on its work in accordance with ASAE 3000 *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*.][71]

[*Assurance Report*]

The format of the report will be in accordance with ASAE 3150 with respect to reasonable assurance engagements [and will be in long-form, including assurance procedures and findings]. An example of the proposed report is contained in the appendix to this letter.

[Our report will be issued [*frequency*] and will cover [*period reported on*].][72]

The reasonable assurance report will be attached to the description of the system [and ABC's Statement] and our opinion will be phrased in terms of [ABC's Statement regarding] the suitability of

[70] Insert if controls which may be material to the engagement are operated by a third party, service or sub-service organisation.
[71] Insert this sentence if the work of internal audit is an integral part of the assurance engagement.
[72] Insert this sentence for recurring engagements.

the design of controls to achieve the control objectives, the fair presentation of the description and the operating effectiveness of controls as designed.

[*Use of the Assurance Report*][73]

[Our report is prepared for the use of ABC and [*intended users*] for [*purpose*] and may not be suitable for any other purpose.

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 ABC and [*intended users*], or for any purpose other than that for which it was prepared.]

[*Material Deficiencies in Design, Misstatements in Description or Deviations in Operating Effectiveness of Controls*]

We will issue an assurance report without modification, to provide a reasonable assurance conclusion on the controls within the [t*ype or name of*] system where our procedures do not identify a material deficiency in the design of controls necessary to achieve the control objectives, misstatement in the description of the [*type or name of*] system by the responsible party, or deviation in the operating effectiveness of controls as designed. For this purpose, a material deviation, misstatement or deficiency exists when:

(a) the controls as designed or the degree of compliance with them will not or may not achieve the control objectives in all material respects or the description contains material inaccuracies, inadequacies or omissions; and

(b) knowledge of that deficiency, misstatement or deviation would be material to users of the assurance report.

If our assurance engagement identifies that there are material deficiencies in the design or deviations in the operating effectiveness of controls during the period covered by the report, such deficiencies or deviations 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 deviations were corrected if that is the case. If any material deficiencies or deviations 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 may also provide you with a letter containing recommendations for strengthening controls if such matters are observed during the process of the assurance engagement. Although issues raised may not represent deficiencies in design or deviations in operating effectiveness of the controls which are material to our conclusion, our 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 controls within the [*the type or name of*] system, including our respective responsibilities.

Yours faithfully,

[73] Insert this section if the report is to be for restricted use only.

(signed)

……

Name and Title

Date

Acknowledged on behalf of [ABC/engaging party]

(signed)

…….

Name and Title

Date

Example 3: Engagement Letter for a Direct Engagement for Reasonable Assurance on the Design and Implementation of Controls

To [the appropriate addressee]:

[*The objective and scope of the engagement*]

You have requested that we undertake a reasonable assurance engagement to report on the design and implementation of ABC's controls[74] over [overall control objectives] within [*the type or name of*] system as at [*date*]. [*The type or name of*] system comprises control objectives and related controls designed to achieve those objectives implemented as at [*date*], for the purpose of reporting to [*identify intended users: the Board of Directors/Regulator/Customers of ABC*]. The control objectives to be addressed with respect to [overall objective/s] [will be developed by us/are specified by legislation/regulation/are: [*list objectives/requirements or identify them by reference*]].

We are pleased to confirm our acceptance and our understanding of this reasonable assurance engagement by means of this letter. Our assurance engagement will be conducted with the objective of expressing an opinion on the suitability of the design of the controls within ABC's [*the type or name of*] system to achieve the stated control objectives and the implementation of those controls as designed as at [*date*].

[*Responsibilities of the assurance practitioner*]

We will conduct our assurance engagement in accordance with Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls*. That standard requires that we comply with ethical requirements applicable to assurance engagements and plan and perform procedures to obtain reasonable assurance about whether, in all material respects, the controls within ABC's [*the type or name of*] system are suitably designed to achieve the control objectives and implemented as designed, in all material respects. We will perform procedures to obtain evidence about the design and implementation of controls. The procedures selected depend on the assurance practitioner's professional judgement, including the assessment of the risks of material deficiencies in the design and/or implementation of the controls.

Because of the inherent limitations of an assurance engagement, together with the inherent limitations of any system of controls there is an unavoidable risk that some deficiencies in the design or implementation of controls may not be detected, even though the engagement is properly planned and performed in accordance with Standards on Assurance Engagements. The system, within which the controls that we will test are designed to operate, will not be examined except to the extent the system is relevant to the achievement of the control objectives. Accordingly, no opinion will be expressed as to the effectiveness of the system of controls as a whole.

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

Our assurance engagement will be conducted on the basis that [the responsible party/ management/ those charged with governance] acknowledge and understand that they have responsibility:

(a) for the identification of risks that threaten achievement of the control objectives identified above;

(b) for design of the system, comprising controls which will mitigate those risks, so that those risks will not prevent achievement of the identified control objectives, and therefore that the control objectives will be achieved;

(c) for implementation of the controls as designed;

[74] If a specific control component is being reported on only, specify that control component, which will depend on the control framework applied and are most commonly control activities, but may also include: the control environment, risk assessment, information and communication or monitoring activities.

(d) 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 and implementation of the controls within ABC's [*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; and

(e) [if controls designed to be operated by a third party, service or sub-service organisation, may be material to the engagement, to obtain either:

(i) a reasonable assurance report on the design and implementation of controls which covers the relevant controls at the third party; or

(ii) access to all information relevant to the design and implementation of those controls, any additional information requested and access to persons from whom to obtain evidence at the third party.][75]

As part of our engagement, we will request from [the responsible party/ management/ those charged with governance] written confirmation concerning representations made to us in connection with the engagement [and written confirmation concerning any representations made by the third party, where material controls implemented at that third party are included in the scope of the engagement].[75]

[*Assurance Approach*]

We will [develop/identify] the control objectives and related controls for [*the type or name of*] system described above.

Our procedures [will/will not] extend to the control objectives and related controls at relevant third parties [to the extent that those controls are necessary to achieve the relevant [control objectives/compliance controls].

Due to the complex nature of internal control, our assurance procedures will not encompass all individual controls at ABC, but will be restricted to an examination of those controls which are designed to achieve the control objectives.

[*Assurance Procedures*]

Our assurance procedures will include:

(a) obtaining an understanding of the control environment of ABC relevant to the [*type or name of*] system;

(b) developing or identifying suitable control objectives;

(c) evaluating the design of specific controls by:

(i) assessing the risks that threaten achievement of the control objectives; and

(ii) evaluating whether the controls as designed are capable of addressing those risks and achieving the related control objectives; and

[75] Insert if controls which may be material to the engagement are operated by a third party, service or sub-service organisation.

(d) evaluating whether the controls have been implemented as designed so that the control objectives are likely to be achieved if the controls operate effectively.

[In undertaking this engagement, we will work closely with ABC's internal audit function and we intend to place reliance on its work in accordance with ASAE 3000 *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*.][76]

[*Assurance Report*]

The format of the report will be in accordance with ASAE 3150 with respect to reasonable assurance engagements [and will be in long-form, including controls designed to achieve each control objective, assurance procedures and findings]. An example of the proposed report is contained in the appendix to this letter.

[*Use of the Assurance Report*][77]

[Our report is prepared for the use of ABC and [*intended users*] for [*purpose*], and may not be suitable for any other purpose.

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 ABC and [*intended users*], or for any purpose other than that for which it was prepared.]

[*Material Deficiencies in Design or Implementation of Controls*]

We will issue an assurance report without modification, to provide a reasonable assurance opinion on the controls within the [*type or name of*] system where our procedures do not identify a material deficiency in the design of controls necessary to achieve the control objectives identified or a material deficiency in the implementation of controls as designed. For this purpose, a material deficiency exists when:

(a) the controls as designed, or implemented will not or may not achieve the control objectives in all material respects; and

(b) knowledge of that deficiency would be material to users of the assurance report.

If our assurance engagement identifies that there are material deficiencies in the design or implementation of controls as at [*date*] covered by the report, such deficiencies will be disclosed in our report. If any material deficiencies disclosed in our report have been corrected subsequent to [*date*] (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 may also provide you with a letter containing recommendations for strengthening controls if such matters are observed during the process of the assurance engagement. Although issues raised may not represent deficiencies in design or implementation of the controls which are material to our opinion, our 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 controls within the [*the type or name of*] system, including our respective responsibilities.

[76] Insert this sentence if the work of internal audit is an integral part of the assurance engagement.
[77] Insert this section if the report is to be for restricted use only.

Yours faithfully,

(signed)
……

Name and Title

Date

Acknowledged on behalf of [engaging party]

(signed)

…….

Name and Title

Date

Appendix 6

(Ref: Para. A118)

EXAMPLE REPRESENTATION LETTERS

Example 1: Representation Letter for an Attestation Engagement on the Design, Description and Operating Effectiveness of Controls

Example 2: Representation Letter for a Direct Engagement on the Design and Implementation of Controls

The following examples of representation letters provided by the responsible party to the assurance practitioner are for guidance only and are not intended to be exhaustive or applicable to all situations.

Example 1: Representation Letter for an Attestation Engagement on the Design, Description and Operating Effectiveness of Controls

[To assurance practitioner]

This representation letter is provided in connection with your [reasonable/limited] assurance engagement to report on ABC's [*the type or name of*] system (the system) for the period [*date*] to [*date*] (period), set forth in ABC's description of the system pages, [*bb-cc*], for the purpose of expressing an [opinion/conclusion] on [ABC's Statement regarding][78] the suitability of the design to achieve the control objectives, fair presentation of the description of the system 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:

The Design, Description and Operating Effectiveness of the System

- We have fulfilled our responsibilities, as set out in the terms of the engagement dated [*date*], for the preparation of the description of the system, pages [*bb-cc*], and ABC's Statement, page [*aa*], including the completeness, accuracy and method of presentation of that description and Statement and we have a reasonable basis for making that Statement.
- We have identified suitable criteria for the evaluation of controls within the [*title name of*] system, including control objectives [developed/provided by ABC/requirement of [*legislation/regulation/other source*]].
- 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 mitigate those risks, so that those risks will not prevent achievement of the control objectives, and therefore the stated control objectives will be achieved.
- The description of the system fairly presents the [title or name of][79] system implemented as at [*date*] and any changes during the period [*date*] to [*date*].
- The controls related to the control objectives stated in the accompanying description operated effectively throughout the period [*date*] to [*date*] to achieve the control objectives.

[78] Insert if the assurance practitioner's conclusion is to be phrased in terms of ABC's statement.
[79] Title or name of the system usually reflects the function or service which the system provides.

Information Provided

- We have provided you with:
    - 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.
    - Additional information that you have requested from us for the purpose of the assurance engagement.
    - Unrestricted access to persons within ABC from whom you determined it necessary to obtain evidence.
- We have disclosed to you the following matters, of which we are aware:
    - All deficiencies in the design of controls to achieve the identified control objectives.
    - All uncorrected misstatements, including omissions, in the description of the system.
    - All instances where controls have not operated effectively as designed, including instances of non-compliance or suspected non-compliance with laws and regulations, fraud or suspected fraud.
    - 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.
    - The identity of any third parties who operate controls on behalf of ABC, which form part of the system, and whether the carve-out method or inclusive method has been used in the description in relation to those controls and related control objectives.

Yours faithfully,

ABC

…… ……
Management Management

Example 2: Representation Letter for a Direct Engagement on the Design and Implementation of Controls

[To assurance practitioner]

This representation letter is provided in connection with your [reasonable/limited] assurance engagement to report on ABC's [*the type or name of*] system (the system) as at [*date*], for the purpose of expressing an [opinion/conclusion] on the suitability of the design to achieve the control objectives identified by [you/legislation/other source] and implementation of controls as designed as at [*date*].

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:

The Design and Implementation of the System

- We have identified the risks that threaten achievement of control objectives [identified/developed by you/ specified by [*legislation/regulation/other source*]] and designed controls to mitigate those risks, so that those risks will not prevent achievement of the control objectives identified, and therefore the stated control objectives will be achieved, if the controls are operated effectively as designed.
- The controls necessary to achieve the control objectives were implemented as designed as at [*date*].

Information Provided

- We have provided you with:
    - 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.
    - Additional information that you have requested from us for the purpose of the assurance engagement.
    - Unrestricted access to persons within ABC from whom you determined it necessary to obtain evidence.
- We have disclosed to you the following matters, of which we are aware :
    - All deficiencies in the design of controls to achieve the identified control objectives;
    - All deficiencies in the implementation of controls as designed;
    - All instances of non-compliance or suspected non-compliance with laws and regulations, fraud or suspected fraud.
    - Any events subsequent to [*date*] up to [*date of the assurance report*] that could have a significant effect on your report.
    - The identity of any third parties who operate controls on behalf of ABC, which form part of the system.

Yours faithfully,

ABC

…… ……
Management Management

Appendix 7

(Ref: Para. A37, A86)

EXAMPLE RESPONSIBLE PARTY'S STATEMENT ON CONTROLS AND SYSTEM DESCRIPTION

Example 1: Responsible Party's or Evaluator's Statement for an Attestation Engagement on the Design, Description and Operating Effectiveness of Controls

Example 2: Responsible Party's Description of the System

The following examples are for use as a guide only, in conjunction with the requirements and application material in this ASAE, and are not intended to be exhaustive or applicable to all situations.

Example 1: Responsible Party's or Evaluator's Statement for an Attestation Engagement on the Design, Description and Operating Effectiveness of Controls

A Statement by ABC is provided to the assurance practitioner in an attestation engagement and either be made available to users by accompanying the assurance report or referenced in the assurance report. (Ref: Para. 17(a), 89(d)(iv))

Statement by ABC on the Design, Description and Operating Effectiveness of Controls over ABC's Cloud Computer Services

The accompanying description has been prepared for clients of ABC's cloud computer services who have a sufficient understanding to consider the description. ABC confirms that:

(a) The accompanying description at pages [*bb-cc*] fairly presents the cloud computer services system (the system) operated for clients throughout the period [*date*] to [*date*], including:

- The types of functions or services provided and, where relevant, locations, including, as appropriate, the nature of the data stored and/or information processed.
- The procedures by which data was recorded and stored and information was processed.
- How the system dealt with significant events and conditions.
- The process used to prepare reports for clients.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed, in the design of the system, would be implemented by clients, 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 ABC alone.
- Identification of any parts of the system which were operated by a third party service organisation (sub-service organisation) on ABC's behalf and whether the description is inclusive or exclusive of the relevant control objectives and controls.
- Other aspects of ABC's 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 clients' information.

- Any changes to the system during the period [*date*] to [*date*].
- Information relevant to the scope of the system being described, without omission or distortion, while acknowledging that the description is prepared to meet the needs of [*specify users*/a broad range of users] and may not, therefore, include every aspect of the system that [other users/each user] may consider important in their 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*], including 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 prevent the stated control objectives from being achieved; and

(iii) The controls were operating effectively as designed, consistently throughout the period [*date*] to [*date*].

.....

Signed on behalf of [management or those charged with governance] of ABC

Date

Example 2: Responsible Party's Description of the System

In both direct and attestation engagements, if the assurance report concludes on a description of the system, then that description is made available to users, ordinarily by accompanying the assurance report. (Ref: Para. 17(j))

Description of ABC's Cloud Computer Services System

Services Provided

ABC provides its clients with cloud computing services, which involves [*describe services provided*].

The System

The stated control objectives and related controls included in this report apply to ABC's operations as they relate only to its cloud computer services. Specifically excluded from this report are controls within individual systems, controls executed at client premises and other services provided by ABC, including [*other related services provided to clients*].

The effectiveness of controls performed by clients of ABC should also be considered as part of the overall system of control relating to ABC's cloud computing services.

[Describe, as appropriate:[80]

- *The procedures by which client data is received, initiated, recorded, processed, corrected, stored as necessary, or transferred to the reports prepared for clients.*
- *How the system dealt with significant events and conditions, other than transactions.*
- *The process used to prepare reports for clients.*

This may include a description of the flow of transactions or a flowchart].[81]

[Controls at Subservice Organisations][82]

[ABC uses [*name of subservice organisation*] to provide [type or name of] services, which form part of the cloud computing services used by ABC clients. The [*type or name of*] services provided by [*subservice organisation*] are [d*escribe the nature of the services provided*]. ABC's description of the system includes ABC's monitoring controls over the operating effectiveness of controls at [*subservice organisation*] and [includes/excludes][83] the relevant control objectives and related controls of [*subservice organisation*].]

Control Objectives and Related Controls

We set out in this report the control objectives and related controls implemented for ABC. 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.

---

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

[81] The description may be presented in various formats such as narratives, flowcharts, tables or graphics.

[82] Insert this section if ABC uses a subservice organisation which performs some of the services provided to clients which use the system.

[83] 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.

The controls which were in operation at ABC throughout the period from [*date*] to [*date*], or during a lesser period where specified, to ensure that the identified control objectives over cloud computing services are achieved were:

Control Objective

[Overall objective: Security/ Confidentiality/ Privacy/ Accessibility and availability/ Data integrity – completeness/ accuracy/ timeliness/ authorisation]

[Specific objective: *list the specific objectives which relate to each overall objective*]

Related Controls

[*List controls in operation during the period relating to each specific control objective.*]

[**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.*][84]

[**Complementary client controls:** *Describe any complementary user entity controls contemplated in the design of the controls.*][85]

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

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

Appendix 8

(Ref: Para. A139)

EXAMPLE ASSURANCE REPORTS ON CONTROLS

Example 1: Limited Assurance Report on Design and Description of the Entity's Controls as at a Specified Date

Example 2: Reasonable Assurance Report on the Design, Description and Operating Effectiveness of the Entity's Controls throughout the Period

Example 3: Reasonable Assurance Report on the Design and Implementation of the Entity's Controls as at a Specified Date

Example 4: Reasonable Assurance Report on the Design and Operating Effectiveness of the Entity's Controls throughout the Period

The following examples of reports are for guidance only and are not intended to be exhaustive or applicable to all situations. They can be applied to both attestation and direct engagements. These examples are short-form reports but may be converted to long-form reports by inclusion of additional information as indicated.

Example 1: Limited Assurance Report on Design and Description of the Entity's Controls as at a Specified Date

Independent Assurance Practitioner's Report

[*Appropriate Addressee*]

Scope

We have undertaken a limited assurance engagement on the design of controls within ABC's [*type or name of*] system (the controls), comprising [*identify system by distinguishing features, boundaries and control components*],[86] as at [*date*] relevant to [[*list overall objectives*]/ the following control objectives: [*list or reference specific control objectives*]][87] and ABC's description of its [*type or name of*] system at pages [*bb-cc*] (the description).[88] The scope of our limited assurance engagement does not include whether the controls were implemented as designed or operated effectively.

ABC's Responsibilities

ABC is responsible for:

(a) the [*functions or services*] within the [*type/name of*] system;

(b) identifying the control objectives;

(c) identifying the risks that threaten achievement of the control objectives;

(d) designing controls to mitigate those risks, so that those risks will not prevent achievement of the identified control objectives; and

[86] Identify system by function or service provided and entity, facility or location. If the scope of the engagement is restricted to certain control components, identify those components. Components may include: the control environment, risk assessment, control activities, information and communication or monitoring activities, or equivalent components defined by control framework applied.

[87] Control objectives are listed if they are not detailed in the entity's description.

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

(e) preparing the description [and Statement][89] at page [*aa*], including the completeness, accuracy and method of presentation of the description [and Statement].[89]

Our Independence and Quality Management

We have complied with the independence and relevant ethical requirements,[*] which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Australian Standard ASQM 1,[#] which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Assurance Practitioner's Responsibilities

Our responsibility is to express a limited assurance conclusion on [ABC's Statement regarding][90] the suitability of the design of controls in the [*type or name of*] system to achieve the identified control objectives and the presentation of ABC's description of the [*type or name of*] system, based on our procedures. We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls* issued by the Auditing and Assurance Standards Board. That standard requires that we comply with relevant ethical requirements and plan and perform our procedures to obtain limited assurance about whether anything has come to our attention that, in all material respects, the controls were not suitably designed to achieve the identified control objectives or the description was not fairly presented as at [*date*].

An assurance engagement to report on the design and description of controls involves performing procedures to obtain evidence about the suitability of the control objectives as criteria to evaluate the controls, the risks that threaten achievement of those objectives, the suitability of the design of the controls to achieve the stated control objectives and the completeness, accuracy and method of presentation of the description of the [*name of*] system as at [date].

In a limited assurance engagement, the assurance practitioner performs procedures, primarily consisting of making enquiries of management and others within the entity, as appropriate, and examination of design specifications or documentation, and evaluates the evidence obtained. The procedures selected depend on our judgement, including the assessment of the risks that the controls are not suitably designed and that the description is not fairly presented. An assurance engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives.

> [*Insert an informative summary of the nature, timing and extent of procedures performed that, in the assurance practitioner's judgement, provides additional information that may be relevant to the users' understanding of the basis for the assurance practitioner's conclusion. The following section has been provided as guidance, and the example procedures are not an exhaustive list of either the type, or extent, of the procedures which may be important for the users' understanding of the work performed.*[91]

---

[89] Insert for attestation engagements if a responsible party's or evaluator's Statement is provided to users.

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

[#] See ASQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements*.

[90] Insert for attestation engagements if the opinion is phrased in terms of the Statement.

[91] The procedures are to be summarised but not to the extent that they are ambiguous, nor described in a way that is overstated or embellished or that implies that reasonable assurance has been obtained. It is important that the description of the procedures does not give the impression that an agreed-upon procedures engagement has been undertaken, and in most cases will not detail the entire work plan.

Given the circumstances of the engagement, in performing the procedures listed above we:

- Through enquiries, obtained an understanding of ABC's control environment and information systems relevant to [*type or name of*] system.
- Through enquiries and inspection, obtained an understanding of how the controls were designed to operate and evaluated whether those controls would be sufficient to achieve each [overall/specific] control objective.
- Assessed whether the description accurately reflected the design of controls identified through the procedures above.][92]

The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement and consequently the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed. Accordingly, we do not express a reasonable assurance opinion on the controls.

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

Limitations of Controls

Because of the inherent limitations of any internal control structure it is possible that, even if the controls are suitably designed, once the controls are in operation the control objectives may not be achieved so that fraud, error, or non-compliance with laws and regulations may occur and not be detected. [Further, the internal control structure, within which the controls that we have assured are designed to operate, has not been assured and no conclusion is expressed on the suitability of its design.][93]

A limited assurance engagement on the design and description of controls at a specified date does not provide assurance on whether the controls were implemented as designed, operated effectively as designed or will operate effectively in the future. Any projection of the outcome of the evaluation of the suitability of the design of controls to future periods is subject to the risk that the controls may become unsuitable because of changes in conditions, or that the degree of compliance with them may deteriorate.

Conclusion

Our limited assurance conclusion has been formed on the basis of the matters outlined in this report.

Based on the procedures we have performed and the evidence we have obtained, nothing has come to our attention that causes us to believe that, in all material respects [ABC's Statement is not fairly presented, in that]:[94]

(a) the controls as at [*date*] were not suitably designed to achieve [[*list overall objectives*]/the control objectives identified]; and

(b) the description does not fairly present the [*the type or name of*] system as at [*date*] as designed.

[92] This section should be deleted if the assurance practitioner concludes that the expanded information on the procedures performed is not needed in the circumstances of the engagement.
[93] Include if only selected components of control have been assured.
[94] Insert for attestation engagements if the conclusion is phrased in terms of ABC's Statement.

[*For a long-form report include a separate section, under an appropriate heading, or reference to an attachment for any additional information agreed in the terms of engagement to be provided to users, for example:*

- Terms of the engagement.
- Criteria being used, such as the specific control objectives and controls designed to achieve each objective.
- Descriptions of the tests of controls that were performed.
- Findings relating to the tests of controls that were performed or particular aspects of the engagement.
- Details of the qualifications and experience of the assurance practitioner and others involved with the engagement.
- Disclosure of materiality levels.
- Recommendations for improvements to controls.]

[*Restricted Use*][95]

[This report has been prepared for use by [*intended users*] for the purpose of [*explain purpose*]. We disclaim any assumption of responsibility for any reliance on this report to any person other than [*intended users*], or for any other purpose other than that for which it was prepared.]

[*Assurance practitioner's signature*][96]

[*Date of the assurance practitioner's assurance report*]

[*Assurance practitioner's address*][97]

[95] Insert section if the report is restricted use.
[96] The assurance practitioner's report needs to be signed in one or more of the following ways: name of the assurance practitioner's firm, name of the assurance practitioner's company or the personal name of the assurance practitioner as appropriate.
[97] The assurance practitioner's address includes the location in the jurisdiction where the assurance practitioner practices.

Example 2: Reasonable Assurance Report on the Design, Description and Operating Effectiveness of the Entity's Controls throughout the Period

Independent Assurance Practitioner's Report

[*Appropriate Addressee*]

Scope

We have undertaken a reasonable assurance engagement on the design of controls within ABC's [*type/name of*] system (the controls), comprising [*identify system by distinguishing features, boundaries and control components*],[98] throughout the period [*date*] to [*date*] relevant to [[*list overall control objectives*]/ the following control objectives: [*list or reference the control objectives*]], ABC's description of its [*type or name of*] system at pages [*bb-cc*] (the description),[99] and the operating effectiveness of those controls.

ABC's Responsibilities

ABC is responsible for:

(a) the [*functions or services*] within the [*type/name of*] system;

(b) identifying the control objectives;

(c) identifying the risks that threaten achievement of the control objectives;

(d) designing controls to mitigate those risks, so that those risks will not prevent achievement of the identified control objectives;

(e) preparing the description [and Statement][100] at page [*aa*], including the completeness, accuracy and method of presentation of the description [and Statement];[101] and

(f) operating those controls effectively as designed throughout the period.

Our Independence and Quality Management

We have complied with the independence and relevant ethical requirements,[*] which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Australian Standard ASQM 1,[#] which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Assurance Practitioner's Responsibilities

Our responsibility is to express an opinion on [ABC's Statement regarding][101] the suitability of the design of controls to achieve the control objectives, the presentation of ABC's description of the [*type or name of*] system and the operating effectiveness of ABC's controls within [*type or name of*] system, based on our procedures. We conducted our engagement in accordance with

---

98 Identify the system by function or service provided and entity, facility or location. If the scope of the engagement is restricted to certain control components, identify those components. Components may include: the control environment, risk assessment, control activities, information and communication or monitoring activities, or equivalent components defined by control framework applied.

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

100 Insert for attestation engagements if the responsible party's or evaluator's Statement is provided to users.

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

\# See ASQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements*.

101 Insert for attestation engagements if the opinion is phrased in terms of the Statement.

Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls* issued by the Auditing and Assurance Standards Board. That standard requires that we comply with relevant ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the controls are suitably designed to achieve the control objectives, the description is fairly presented and the controls operated effectively throughout the period.

An assurance engagement to report on the design, description and operating effectiveness of controls involves performing procedures to obtain evidence about the suitability of the design of controls to achieve the control objectives, the completeness, accuracy and method of presentation of the description of the [*name of*] system and the operating effectiveness of controls throughout the period. The procedures selected depend on our judgement, including the assessment of the risks that the controls are not suitably designed, the description is not fairly presented or the controls did not operate effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to achieve the control objectives stated in the description. An assurance engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives.

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

Limitations of Controls

Because of the inherent limitations of any internal control structure it is possible that, even if the controls are suitably designed and operating effectively, the control objectives may not be achieved so that fraud, error, or non-compliance with laws and regulations may occur and not be detected. [Further, the internal control structure, within which the controls that we have assured are designed to operate, has not been assured and no opinion is expressed as to its design or operating effectiveness.][102]

An assurance engagement on the operating effectiveness of controls is not designed to detect all instances of controls operating ineffectively as it is not performed continuously throughout the period and the tests performed are on a sample basis. Any projection of the outcome of the evaluation of controls to future periods is subject to the risk that the controls may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report.

In our opinion, in all material respects [ABC's Statement is fairly presented, in that]:[103]

(a) the controls were suitably designed to achieve [[*list overall objectives*]/ the control objectives identified] throughout the period [*date*] to [*date*];

(b) the description fairly presents the [*type or name of*] system as designed, throughout the period [*date*] to [*date*]; and

(c) the controls, necessary to achieve the control objectives, operated effectively as designed, throughout the period from [*date*] to [*date*].

[102] Include if only selected components of control have been assured.
[103] Insert for attestation engagements if the opinion is phrased in terms of ABC's Statement.

[*For a long-form report, include a separate section, under an appropriate heading, or reference to an attachment for any additional information agreed in the terms of engagement to be provided to users, for example:*

- Terms of the engagement.
- Criteria being used, such as the specific control objectives and controls designed to achieve each objective.
- Descriptions of the tests of controls that were performed.
- Findings relating to the tests of controls that were performed or particular aspects of the engagement.
- Details of the qualifications and experience of the assurance practitioner and others involved with the engagement.
- Disclosure of materiality levels.
- Recommendations for improvements to controls.]

[*Restricted Use*][104]

[This report has been prepared for use by [*intended users*] for the purpose of [*explain purpose*]. We disclaim any assumption of responsibility for any reliance on this report to any person other than [*intended users*], or for any other purpose other than that for which it was prepared.]

[*Assurance practitioner's signature*]

[*Date of the assurance practitioner's assurance report*]

[*Assurance practitioner's address*]

[104] Insert section if the report is restricted use.

Example 3: Reasonable Assurance Report on the Design and Implementation of the Entity's Controls as at a Specified Date

Independent Assurance Practitioner's Report

[*Appropriate Addressee*]

Scope

We have undertaken a reasonable assurance engagement on the design and implementation of controls within ABC's [*type/name of*] system (the controls), comprising [*identify system by distinguishing features, boundaries and control components*][105] as at [*date*] relevant to [[*list overall objectives*]/ the following control objectives: [*List or reference the control objectives*]][106]

ABC's Responsibilities

ABC is responsible for:

(a) the [*functions or services*] within the [*type/name of*] system;

(b) identifying the control objectives;

(c) identifying the risks that threaten achievement of the control objectives;

(d) designing controls to mitigate those risks, so that those risks will not prevent achievement of the identified control objectives;

(e) implementing the controls as designed; and

(f) [preparing the accompanying Statement at page [*aa*], including the completeness, accuracy and method of presentation of the Statement.][107]

Our Independence and Quality Management

We have complied with the independence and relevant ethical requirements,[*] which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Australian Standard ASQM 1,[#] which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Assurance Practitioner's Responsibilities

Our responsibility is to express an opinion on [ABC's Statement regarding][108] the suitability of the design to achieve the control objectives and implementation as designed, of ABC's controls within [*type or name of*] system based on our procedures. We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls* issued by the Auditing and Assurance Standards Board. That standard requires that we

---

[105] Identify the system by function or service provided and entity, facility or location. If the scope of the engagement is restricted to certain control components, identify those components. Components may include: the control environment, risk assessment, control activities, information and communication or monitoring activities, or equivalent components defined by control framework applied.

[106] Either list overall control objectives or list specified control objectives depending on scope of engagement.

[107] Insert for attestation engagements if the responsible party's or evaluator's Statement is provided to users.

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

[#] See ASQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements*.

[108] Insert for attestation engagements if the opinion is phrased in terms of the Statement.

comply with relevant ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the controls are suitably designed to achieve the control objectives and the controls, necessary to achieve the control objectives, were implemented as designed as at [*date*].

An assurance engagement to report on the design and implementation of controls involves performing procedures to obtain evidence about the suitability of the design of controls to achieve the control objectives and the implementation of those controls as designed as at [date]. The procedures selected depend on our judgement, including the assessment of the risks that controls are not suitably designed or implemented as designed. Our procedures included testing the implementation of those controls that we consider necessary to achieve the control objectives identified. An assurance engagement of this type also includes evaluating the suitability of the control objectives.

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

Limitations of Controls

Because of the inherent limitations of any internal control structure it is possible that, even if the controls are suitably designed and implemented as designed, once the controls are in operation the control objectives may not be achieved so that fraud, error, or non-compliance with laws and regulations may occur and not be detected. [Further, the internal control structure, within which the controls that we have assured are designed to operate, has not been assured and no opinion is expressed as to its design or implementation.][109]

An assurance engagement on the implementation of controls at a specified date does not provide assurance on whether the controls operated effectively as designed or will operate effectively in the future. Any projection of the outcome of the evaluation of the suitability of the design of controls to future periods is subject to the risk that the controls may become unsuitable because of changes in conditions.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report.

In our opinion, in all material respects [ABC's Statement is fairly presented, in that]:[110]

(a) the controls within the [*the type or name of*] system were suitably designed as at [*date*] to achieve [[*list overall objectives*]/ the control objectives identified]; and

(b) the controls were implemented as designed as at [*date*].

[*For a long-form report, include a separate section, under an appropriate heading, or reference to an attachment for any additional information agreed in the terms of engagement to be provided to users, for example:*

- Terms of the engagement.
- Criteria being used, such as the specific control objectives and controls designed to achieve each objective.
- Descriptions of the tests of controls that were performed.
- Findings relating to the tests of controls that were performed or particular aspects of the engagement.

[109] Include if only selected components of control have been assured.
[110] Insert for attestation engagements if the opinion is phrased in terms of the Statement.

- Details of the qualifications and experience of the assurance practitioner and others involved with the engagement.
- Disclosure of materiality levels.
- Recommendations for improvements to controls.]

[*Restricted Use*][111]

[This report has been prepared for use by [*intended users*] for the purpose of [*explain purpose*]. We disclaim any assumption of responsibility for any reliance on this report to any person other than [*intended users*], or for any other purpose other than that for which it was prepared.]

[*Assurance practitioner's signature*]

[*Date of the assurance practitioner's assurance report*]

[*Assurance practitioner's address*]

[111] Insert section if the report is restricted use.

Example 4: Reasonable Assurance Report on the Design and Operating Effectiveness of the Entity's Controls throughout the Period

Independent Assurance Practitioner's Report

[*Appropriate Addressee*]

Scope

We have undertaken a reasonable assurance engagement on the design and the operating effectiveness of controls within ABC's [*type/name of*] system (the controls), comprising [*identify system by distinguishing features, boundaries and control components*],[112] throughout the period [*date*] to [*date*]] relevant to [[*list overall objectives*]/ the following control objectives: [*List or reference the control objectives*]][113]

ABC's Responsibilities

ABC is responsible for:

(a) the [*functions or services*] within the [*type/name of*] system;

(b) identifying the control objectives;

(c) identifying the risks that threaten achievement of the control objectives;

(d) designing controls to mitigate those risks, so that those risks will not prevent achievement of the identified control objectives;

(e) operating effectively the controls as designed throughout the period; and

(f) [preparing the accompanying Statement at page [*aa*], including the completeness, accuracy and method of presentation of the Statement.][114]

Our Independence and Quality Management

We have complied with the independence and relevant ethical requirements,[*] which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Australian Standard ASQM 1,[#] which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Assurance Practitioner's Responsibilities

Our responsibility is to express an opinion on [ABC's Statement regarding][115] the suitability of the design to achieve the control objectives and operating effectiveness of ABC's controls within [*type or name of*] system, based on our procedures. We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls* issued by the Auditing and Assurance Standards Board. That standard requires that we

---

[112] Identify the system by function or service provided and entity, facility or location. If the scope of the engagement is restricted to certain control components, identify those components. Components may include: the control environment, risk assessment, control activities, information and communication or monitoring activities, or equivalent components defined by control framework applied.

[113] Either list overall control objectives or list specified control objectives depending on scope of engagement.

[114] Insert for attestation engagements if the responsible party's or evaluator's Statement is provided to users.

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

[#] See ASQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements*.

[115] Insert for attestation engagements if the opinion is phrased in terms of the Statement.

comply with relevant ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the controls are suitably designed to achieve the control objectives and the controls operated effectively throughout the period.

An assurance engagement to report on the design and operating effectiveness of controls involves performing procedures to obtain evidence about the suitability of the design of controls to achieve the control objectives and the operating effectiveness of controls throughout the period. The procedures selected depend on our judgement, including the assessment of the risks that the controls are not suitably designed or the controls did not operate effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to achieve the control objectives identified. An assurance engagement of this type also includes evaluating the suitability of the control objectives.

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

Limitations of Controls

Because of the inherent limitations of any internal control structure it is possible that, even if the controls are suitably designed and operating effectively, the control objectives may not be achieved and so fraud, error, or non-compliance with laws and regulations may occur and not be detected. [Further, the internal control structure, within which the controls that we have assured operate, has not been assured and no opinion is expressed as to its design or operating effectiveness.][116]

An assurance engagement on operating effectiveness of controls is not designed to detect all instances of controls operating ineffectively as it is not performed continuously throughout the period and the tests performed are on a sample basis. Any projection of the outcome of the evaluation of controls to future periods is subject to the risk that the controls may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report.

In our opinion, in all material respects [ABC's Statement is fairly presented, in that]:[117]

(a) the controls within the [*the type or name of*] system were suitably designed to achieve [[*list overall objectives*]/the control objectives identified]; and

(b) the controls operated effectively as designed throughout the period from [*date*] to [*date*].

[*For a long-form report, include a separate section, under an appropriate heading, or reference to an attachment for any additional information agreed in the terms of engagement to be provided to users, for example:*

- Terms of the engagement.
- Criteria being used, such as the specific control objectives and controls designed to achieve each objective.
- Descriptions of the tests of controls that were performed.

[116] Include if only selected components of control have been assured.
[117] Insert for attestation engagements if the opinion is phrased in terms of the Statement.

- Findings relating to the tests of controls that were performed or particular aspects of the engagement.
- Details of the qualifications and experience of the assurance practitioner and others involved with the engagement.
- Disclosure of materiality levels.
- Recommendations for improvements to controls.]

[*Restricted Use*][118]

[This report has been prepared for use by [*intended users*] for the purpose of [*explain purpose*]. We disclaim any assumption of responsibility for any reliance on this report to any person other than [*intended users*], or for any other purpose other than that for which it was prepared.]

[*Assurance practitioner's signature*]

[*Date of the assurance practitioner's assurance report*]

[*Assurance practitioner's address*]

[118] Insert section if the report is restricted use.

Appendix 9

(Ref: Para. A146)

EXAMPLE MODIFIED REASONABLE ASSURANCE REPORTS ON CONTROLS

Example 1: Qualified reasonable assurance opinion – ABC's description of the system is not fairly presented in all material respects

Example 2: Qualified reasonable assurance opinion – the controls are not suitably designed to achieve the control objectives

Example 3: Qualified reasonable assurance opinion – the controls did not operate effectively throughout the period

Example 4: Adverse reasonable assurance opinion – the controls did not operate effectively throughout the period

Example 5: Qualified reasonable assurance opinion – the assurance practitioner is unable to obtain sufficient appropriate evidence of the operation of controls

Example 6: Disclaimer of reasonable assurance opinion – the assurance practitioner is unable to obtain sufficient appropriate evidence of the operation of controls

The following examples of modified reasonable assurance 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 8 and may be adapted for limited assurance conclusions.

Example 1: Qualified reasonable assurance opinion – ABC's description of the system is not fairly presented in all material respects

…

Assurance Practitioner'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 ABC's [*the type or name of system*] system includes the following control/s: [*control/s description/s*]. Based on our procedures, which included enquiries of staff personnel and observation of activities, we have determined that these controls were not fairly presented in the description in that: [*describe omissions, distortions or other inaccuracies in the description*].

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 the control objectives identified in ABC's description of the system at page [*aa*]. In our opinion, in all material respects:

(a) the controls within the system were suitably designed to achieve [[*list overall objectives*]/the control objectives identified];

(b) except for the matter described in the Basis for Qualified Opinion paragraph, the description of the system is fairly presented; and

(c) [*if applicable insert:* the controls were implemented as designed; or]

(d) [*if applicable insert:* the controls operated effectively as designed;]

[as at [*date*]/ throughout the period from [*date*] to [*date*]].

…

Example 2: Qualified reasonable assurance opinion – the controls are not suitably designed to achieve the control objectives

…

Assurance Practitioner'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 control objective: [*control objective*] is designed by ABC to be achieved by [*description of control*]. To achieve the control objective/s identified, ABC's controls would also need to include [*describe control omitted*].

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 the control objectives listed [above/in ABC's description of the system at page [*aa*]]. In our opinion, in all material respects:

(a) except for the matter described in the Basis for Qualified Opinion paragraph, the controls within the system were suitably designed to achieve [[*list overall objectives*]/the control objectives identified]; and

(b) with respect to the controls which were suitably designed only:

  (i) [*if applicable insert:* the description of the system is fairly presented; and/or]

  (ii) [*if applicable insert:* the controls were implemented as designed; or]

  (iii) [*if applicable insert:* the controls operated effectively as designed;]

  [as at [*date*]/throughout the period from [*date*] to [*date*]].

…

Example 3: Qualified reasonable assurance opinion – the controls did not operate effectively throughout the period

…

Assurance Practitioner'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 control objective: [*control objective*] is designed by ABC to be achieved by [*description of control*]. However, this control was not operating effectively during the period from [date] to [*date*] due to [*reason*]. Consequently, we were unable to obtain sufficient assurance that the control objective was achieved during the period from [*date*] to [*date*]. [ABC corrected the operation of the control as of [*date*], and our assurance procedures indicate that it was operating effectively during the period from [*date*] to [*date*].][119]

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 the control objectives described listed [above/in ABC's description of the system at page [*aa*]]. In our opinion, in all material respects:

(a) the controls within the system were suitably designed to achieve [[*list overall objectives*]/the control objectives identified];

(b) [*if applicable insert:* the description of the system is fairly presented;] and

(c) except for the matter described in the Basis for Qualified Opinion paragraph, the controls operated effectively as designed throughout the period from [*date*] to [*date*]].

…

Example 4: Adverse reasonable assurance opinion – the controls did not operate effectively throughout the period

…

Assurance Practitioner's Responsibilities

…

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

Basis for Adverse Opinion

The controls were not operating effectively during the period from [*date*] to [*date*] due to [*reason*]. This resulted in insufficient assurance that the control objectives were achieved during the period from [*date*] to [*date*].

[119] Insert if operation of the control was corrected during the period.

Adverse 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 the control objectives described [above/ in ABC's description of the system at page [*aa*]]. In our opinion, the controls did not operate effectively as designed throughout the period from [*date*] to [*date*]], even though the controls within the system were suitably designed to achieve [[*list overall objectives*]/the control objectives identified] and [*if applicable insert:* the description of the system is fairly presented] in all material respects.

…

Example 5: Qualified reasonable assurance opinion – the assurance practitioner is unable to obtain sufficient appropriate evidence of the operation of controls

…

Assurance Practitioner'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 control objective: [*control objective*] is designed by ABC to be achieved by [*description of control*]. However, insufficient records were available from [*date*] to [*date*] due to [*reason*], and we were therefore unable to test the operation of this control for that period. Consequently, we were unable to determine whether the controls designed to achieve the stated control objective operated 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 listed [above/in ABC's description of the system at page [*aa*]]. In our opinion,

(a) the controls within the system were suitably designed to achieve [[*list overall objectives*]/the control objectives identified];

(b) [*if applicable insert:* the description of the system is fairly presented;] and

(c) except for the matter described in the Basis for Qualified Opinion paragraph, the controls operated effectively as designed throughout the period from [*date*] to [*date*]].

…

Example 6: Disclaimer of reasonable assurance opinion – the assurance practitioner is unable to obtain sufficient appropriate evidence of the operation of controls

…

Assurance Practitioner's Responsibilities

…

Because of the matters described in the Basis for Disclaimer of Opinion paragraph, however, we are not able to obtain sufficient appropriate evidence to provide a basis for a reasonable assurance opinion on the operating effectiveness of controls during the period.

Basis for Disclaimer of Opinion

We were appointed on [*date*] to provide assurance on the design and operation of ABC's controls within the [*type/name of*] system[120] (the controls), throughout the period [*date*] to [*date*]] [relevant to [*list overall objectives*]. However, the date of our appointment was after the end of the period so we were unable to conduct testing of controls whilst they were in operation or walk-throughs during the relevant period, which would be necessary to form an opinion on whether the controls were operating effectively during that period.

Disclaimer of Opinion on the Operating Effectiveness of Controls

Because of the significance of the matter described in the Basis for Disclaimer of Opinion section of our report, we have not been able to obtain sufficient appropriate evidence to provide the basis for an opinion on the operating effectiveness of controls. Accordingly, we do not express an opinion on the operating effectiveness of those controls.

Opinion on the Design of Controls

Our opinion on the design of the controls has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion were those described listed [above/in ABC's description of the system at page [*aa*]]. In our opinion, the controls within the system were suitably designed as at [*date*] to achieve [[*list overall objectives*]/the control objectives identified].

…

[120] Identify system by function or service provided and entity, facility or location boundaries.